ESET FILE SECURITY

PARA MICROSOFT WINDOWS SERVER

Manual de instalação e Guia do usuário

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Clique aqui para fazer download da versão mais recente deste documento

ESET **FILE SECURITY**

Atendimento ao cliente: www.eset.com/support

REV. 11/11/2013

Índice

1. Introdução

O ESET File Security é uma solução integrada especialmente projetada para o ambiente Microsoft Windows Server. O ESET File Security oferece uma proteção forte e eficaz contra vários tipos de ataques de códigos maliciosos. Antivírus e Antispyware.

Eis alguns dos principais recursos do ESET File Security:

- Exclusões automáticas - detecção e exclusão automática de arquivos críticos do servidor, para um funcionamento perfeito.
- eShell (ESET Shell) - nova interface de controle de linha de comando que oferece aos usuários avançados e administradores opções mais abrangentes para o gerenciamento de produtos da ESET.
- Autodefesa - tecnologia que protege as soluções de segurança da ESET de serem alteradas ou desativadas.
- Solução de problemas eficaz - com ferramentas avançadas incorporadas para solucionar vários problemas: ESET SysInspector para diagnósticos do sistema e ESET SysRescue para criar um CD de recuperação inicializável.

O ESET File Security suporta as versões autônomas 2000, 2003 e 2008 do Microsoft Windows Server, bem como o Microsoft Windows Server em um ambiente de agrupamento. É possível gerenciar remotamente o ESET File Security em grandes redes com a ajuda do ESET Remote Administrator.

1.1 Requisitos do sistema

Sistemas operacionais compatíveis:

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 e x64)
- Microsoft Windows Server 2008 (x86 e x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Storage Server 2008 R2 Essentials SP1
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Os requisitos de hardware dependem da versão do sistema operacional em uso. Recomendamos ler a documentação do Microsoft Windows Server para obter informações mais detalhadas sobre os requisitos de hardware.

1.2 Tipos de proteção

Há dois tipos de proteção:

- Proteção antivírus
- Proteção antispyware

A proteção antivírus e antispyware é uma das funções básicas do produto ESET File Security. Ela protege contra ataques de sistemas maliciosos ao controlar arquivos, emails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

1.3 Interface do usuário

O ESET File Security tem uma interface gráfica de usuário (GUI) projetada para ser o mais intuitiva possível. A GUI permite que os usuários acessem rápida e facilmente as principais funções do programa.

Além da GUI principal, há uma **árvore de configuração avançada** acessível em qualquer local do programa, pressionando a tecla F5.

Ao pressionar F5, a janela da árvore de configuração avançada se abre e exibe uma lista dos recursos do programa que podem ser configurados. Nessa janela, você pode configurar os ajustes e opções com base em suas necessidades. A estrutura em árvore divide-se em duas seções: **Proteção do servidor** e **Proteção do computador**. A seção **Proteção do servidor** contém Exclusões automáticas, específicas para o sistema operacional e os arquivos de sistema do servidor. A seção **Proteção do computador** contém os itens configuráveis para a proteção do computador.

2. Instalação

Após comprar o ESET File Security, o instalador pode ser transferido do site da ESET (www.eset.com) em um pacote .msi.

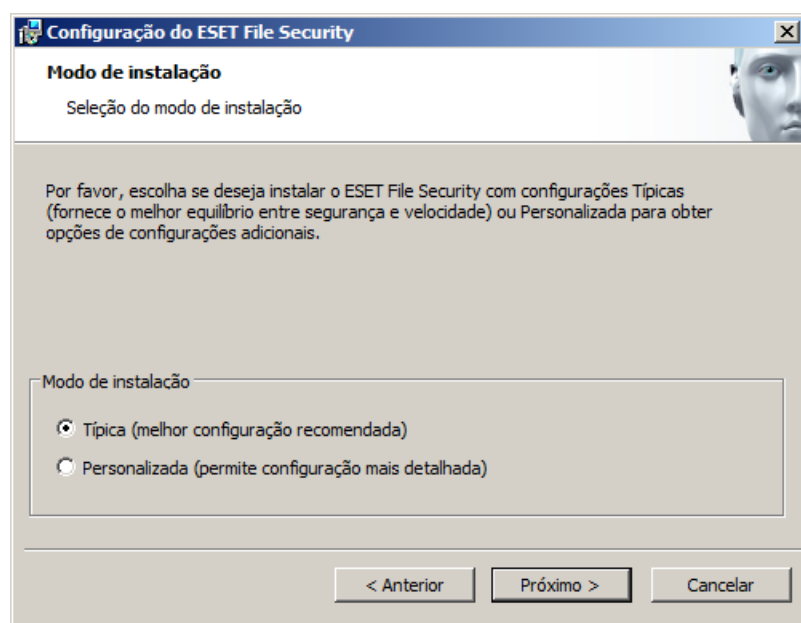
Observe que você precisa executar o instalador na conta **Administrador incorporado**. Qualquer outro usuário, apesar de ser membro do grupo de administradores, não terá direitos de acesso suficientes. Portanto, é necessário usar a conta de administrador incorporado, pois você não poderá concluir a instalação com êxito em qualquer outra conta de usuário que não seja **Administrador**.

Há duas maneiras de executar o instalador:

- Você pode fazer login localmente usando as credenciais de conta do Administrador e simplesmente ao executar o instalador
- Você pode se conectar como outro usuário, mas precisa abrir o aviso de comando com **Executar como...** e digitar as credenciais de conta de Administrador para ter o cmd executando como Administrador e então digitar o comando para executar o instalador (p. ex., `msiexec /i efsw_nt64_ENU.msi` mas você precisa substituir `efsw_nt64_ENU.msi` pelo nome de arquivo exato do instalador msi que você baixou)

Após o início do instalador, o assistente de instalação o guiará pela configuração básica. Há dois tipos de instalação disponíveis com diferentes níveis de detalhes de configuração:

1. **Instalação típica**

2. **Instalação personalizada**

OBSERVAÇÃO: Recomendamos que instale o ESET File Security em um SO instalado e configurado recentemente, se possível. No entanto, se precisar instalá-lo em um sistema existente, o melhor a fazer é desinstalar a versão anterior do ESET File Security, reiniciar o servidor e instalar o novo ESET File Security em seguida.

2.1 Instalação típica

O modo de instalação Típica instala rapidamente o ESET File Security com a configuração mínima durante o processo de instalação. A instalação típica é o modo de instalação padrão e é recomendada se você ainda não tiver requisitos particulares para configurações específicas. Após a instalação do ESET File Security no sistema, é possível modificar as opções e configurações a qualquer momento. Este guia do usuário descreve essas configurações e recursos em detalhes. As configurações do modo de instalação Típica proporcionam excelente segurança, facilidade de uso e alto desempenho do sistema.

Após selecionar o modo de instalação e clicar em Avançar, você será solicitado a inserir o nome de usuário e a senha. Essa etapa tem um papel significativo no fornecimento de proteção constante ao seu sistema, pois o nome de usuário e a senha permitem as Atualizações automáticas do banco de dados de assinatura de vírus.

Insira o nome de usuário e a senha recebidos após a compra ou registro do produto, nos campos correspondentes.

Caso você não tenha o nome de usuário e a senha disponíveis no momento, eles poderão ser inseridos diretamente no programa posteriormente.

Na próxima etapa - **Gerenciador de licenças** - Adicione o arquivo de licença que foi enviado por email após a compra do produto.

A próxima etapa é configurar o ThreatSense.Net Early Warning System. O ThreatSense.Net Early Warning System ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar ThreatSense.Net Early Warning System** é selecionada. Clique em **Configuração avançada...** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos.

A próxima etapa do processo de instalação é a configuração da **Detecção de aplicativos potencialmente não desejados**. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Para obter mais detalhes, consulte o capítulo Aplicativos potencialmente não desejados.

Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Selecione a opção **Ativar detecção de aplicativos potencialmente não desejados** para permitir que o ESET File Security detecte esse tipo de aplicativos. Se não desejar ativar esse recurso, selecione **Desativar detecção de aplicativos potencialmente não desejados**.

A última etapa no modo de instalação Típica é confirmar a instalação clicando no botão **Instalar**.

2.2 Instalação personalizada

A instalação personalizada foi desenvolvida para os usuários que desejam configurar o ESET File Security durante o processo de instalação.

Após selecionar o modo de instalação e clicar em **Avançar**, será exibida a solicitação para que você selecione um local de destino para a instalação. Por padrão, o programa é instalado em *C:\Program Files\ESET\ESET File Security*. Clique em **Procurar...** para alterar este local (não recomendado).

Em seguida, insira o **Nome de usuário** e **Senha**. Esta etapa é a mesma que no modo de instalação típica (consulte "Instalação típica").

Na próxima etapa - **Gerenciador de licenças** – adicione o arquivo de licença que foi enviado por email após a compra do produto.

Após a inserção do nome de usuário e da senha, clique em **Avançar** para passar para **Configurar sua conexão com a Internet**.

Se estiver usando um servidor proxy, ele deve estar configurado corretamente para que as atualizações do banco de dados de assinatura de vírus funcionem corretamente. Se desejar que o servidor proxy seja configurado automaticamente, selecione a configuração padrão **Não tenho certeza se minha conexão com a Internet utiliza um servidor proxy. Use as mesmas configurações usadas pelo Internet Explorer (Recomendável)** e clique em **Avançar**. Se não estiver usando um servidor proxy, selecione a opção **Eu não utilizo um servidor proxy**.

Se preferir digitar os detalhes do servidor proxy, poderá configurá-lo manualmente. Para configurar os ajustes do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Avançar**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **Nome de usuário** e uma **Senha** válidos a fim de obter acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Após inserir os detalhes do servidor proxy, clique em **Aplicar** e confirme a seleção.

Clique em **Avançar** para prosseguir para **Configurar definições de atualização automática**. Esta etapa permite definir se deseja que as atualizações de componentes sejam ou não automáticas no seu sistema. Clique em **Alterar...** para acessar as configurações avançadas.

Se não desejar atualizar os componentes do programa, selecione a opção **Nunca atualizar componentes de programa**. Selecione a opção **Perguntar antes de fazer download dos componentes do programa** para exibir uma janela de confirmação antes de fazer download dos componentes de programa. Para fazer o download dos componentes do programa automaticamente, selecione a opção **Sempre atualizar componentes do programa**.

OBSERVAÇÃO: Após a atualização de um componente do programa, geralmente é necessário reiniciar o computador. Recomendamos selecionar a opção **Nunca reiniciar o computador**. As atualizações de componentes mais recentes entrarão em vigor após a próxima reinicialização do servidor agendada, manual ou outra). Você pode escolher **Sugerir opção de reinicialização do computador, se necessário** caso queira ser lembrado de reiniciar o

servidor após a atualização dos componentes. Com esta configuração, você pode reiniciar o servidor na hora ou adiar a reinicialização e fazer isto posteriormente.

A próxima janela de instalação oferece a opção de definir uma senha para proteger as configurações do programa. Selecione a opção **Proteger as configurações por senha** e digite a senha nos campos **Nova senha** e **Confirmar nova senha**.

As próximas duas etapas da instalação, **ThreatSense.Net Early Warning System** e **Detecção de aplicativos potencialmente não desejados** são as mesmas etapas no modo de instalação Típica (consulte "Instalação típica").

Clique em **Instalar** na janela **Pronto para instalar** para concluir a instalação.

2.3 Servidor de terminal

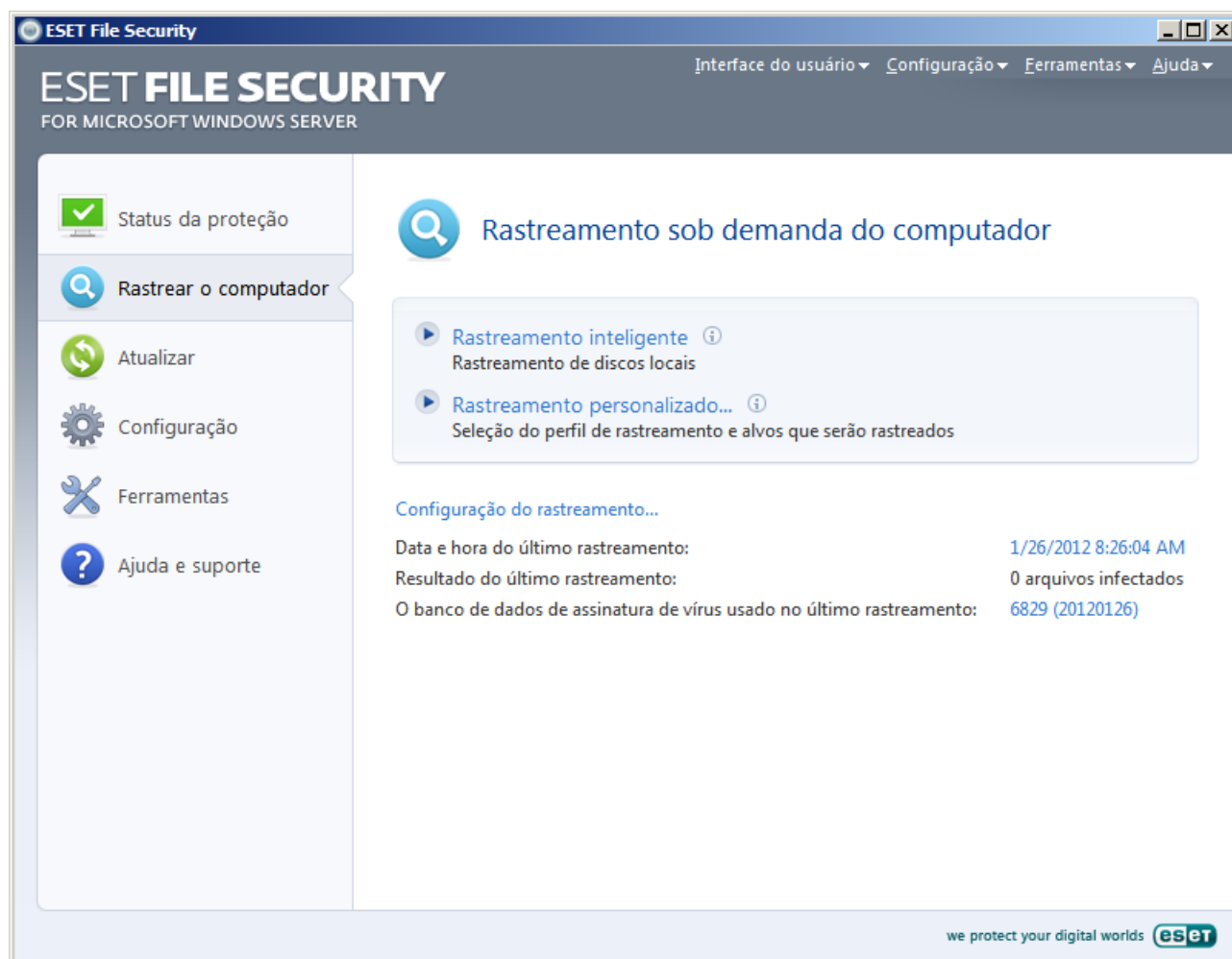
Se o ESET File Security estiver instalado em Windows Server que atue como Servidor de terminal, você pode desejar desativar a GUI do ESET File Security para evitar que ela inicie todas as vezes em que um usuário fizer login. Consulte o capítulo Desativar a GUI no servidor de terminal para conhecer as etapas específicas para desativá-la.

2.4 Atualização para uma versão mais recente

As novas versões do ESET File Security foram lançadas para proporcionar melhorias ou consertar problemas que não podiam ser resolvidos por atualizações automáticas do módulo do programa. Para fazer a atualização para uma nova versão, faça o seguinte:

1. Atualizar automaticamente por meio de uma atualização dos componentes do programa (PCU)
   Já que as atualizações dos componentes do programa são distribuídas a todos os usuários e podem ter um impacto em determinadas configurações do sistema, geralmente são lançadas após um longo período de testes, a fim de garantir um processo de atualização tranquilo em todas as configurações de sistema possíveis. Se precisar atualizar para uma versão mais recente imediatamente após seu lançamento, use um dos métodos a seguir.
2. Atualizar manualmente por meio de download e instalação de uma nova versão sobre a instalação anterior
   No início da instalação, é possível optar por preservar as configurações atuais do programa marcando a caixa de seleção **Utilizar configurações atuais**.
3. Atualizar manualmente com implementação automática em um ambiente de rede por meio do ESET Remote Administrator.

2.5 Rastreamento sob demanda do computador

Após instalar o ESET File Security, deverá ser executado um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastrear o computador** e, em seguida, em **Rastreamento inteligente**. Para obter mais informações sobre os rastreamentos sob demanda do computador, consulte a seção Rastreamento sob demanda do computador.

3. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET File Security e de suas configurações básicas.

3.1 Introdução ao design da interface do usuário

A janela principal do ESET File Security é dividida em duas seções principais. A janela principal à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

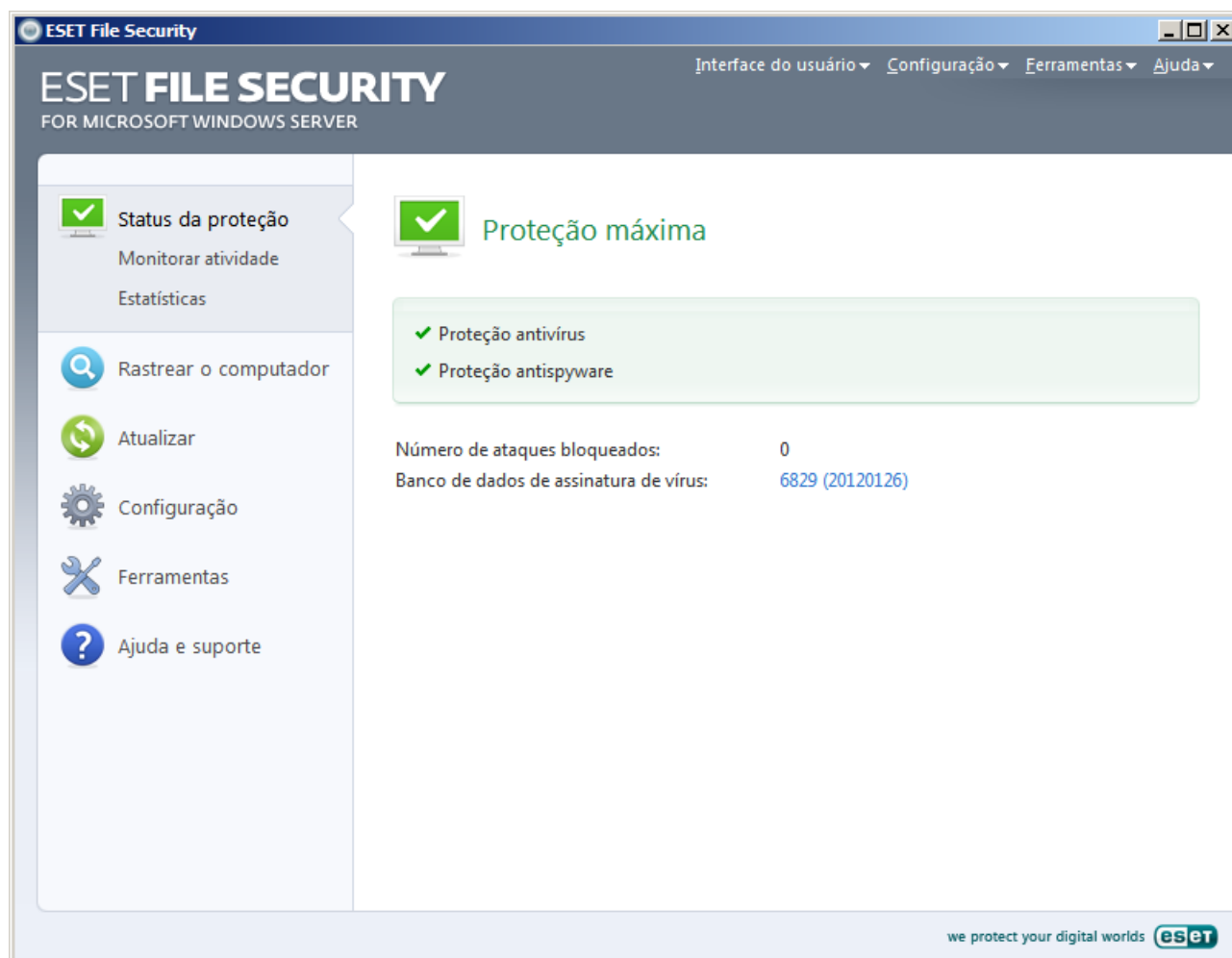
Status da proteção - Fornece informações sobre o status da proteção do ESET File Security. Se o modo Avançado estiver ativado, serão exibidos os submenus **Monitorar atividade** e **Estatísticas**.

Rastrear o computador - Esta opção permite configurar e iniciar o rastreamento Sob Demanda do computador.

Atualizar - Exibe informações sobre as atualizações do banco de dados de assinatura de vírus.

Configuração - Selecione esta opção para ajustar o nível de segurança do seu computador. Se o modo Avançado estiver ativado, o submenu **Antivírus e antispyware** será exibido.

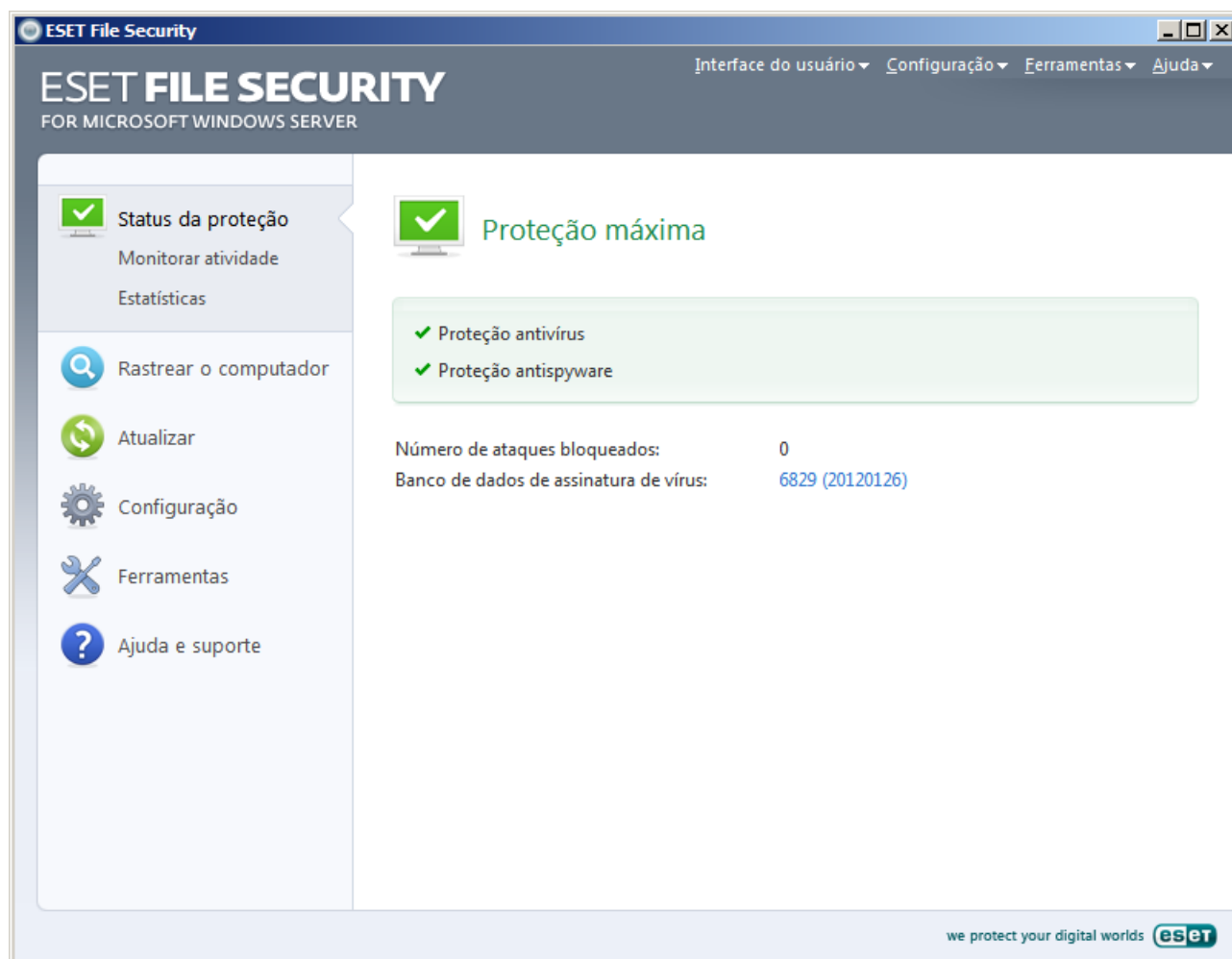
Ferramentas - Fornece o acesso a **Relatórios**, **Quarentena**, **Agenda** e **SysInspector**. Esta opção é exibida somente no modo Avançado.

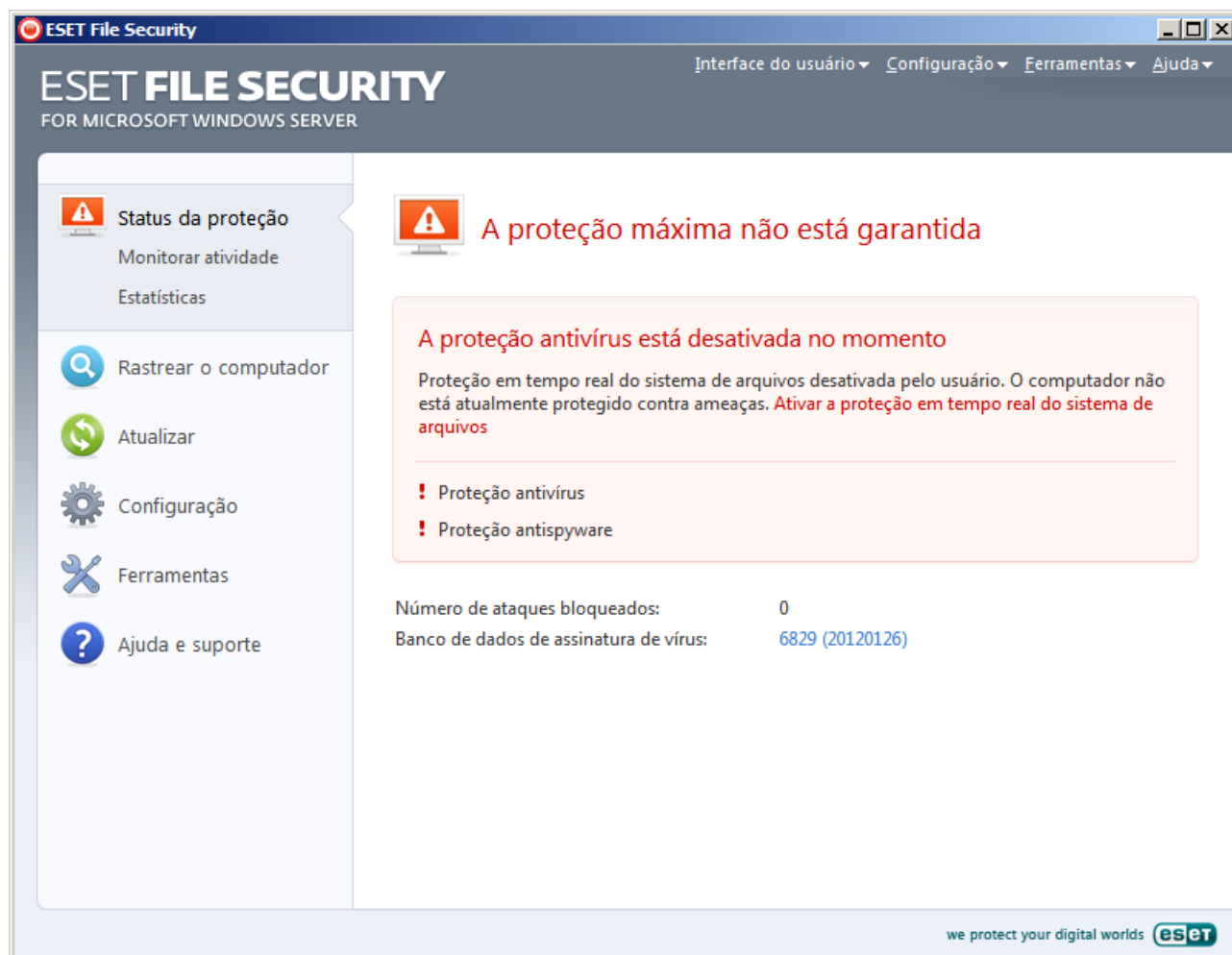
Ajuda e suporte - Fornece acesso a arquivos de ajuda, ao banco de dados de conhecimento da ESET, ao site da ESET e a links para abrir uma solicitação de suporte no Atendimento ao cliente.

3.1.1 Verificação do funcionamento do sistema

Para exibir o **Status da proteção**, clique na opção superior do menu principal. Um resumo de status sobre o funcionamento do ESET File Security será exibido na janela primária, e será exibido um submenu com duas opções. **Monitorar atividade** e **Estatísticas**. Selecione uma das opções para visualizar informações mais detalhadas sobre o sistema.

Quando o ESET File Security for executado com o recurso completo, o **Status da proteção** aparecerá na cor verde. Caso contrário, fica em vermelho ou laranja, o que significa que requer sua atenção.

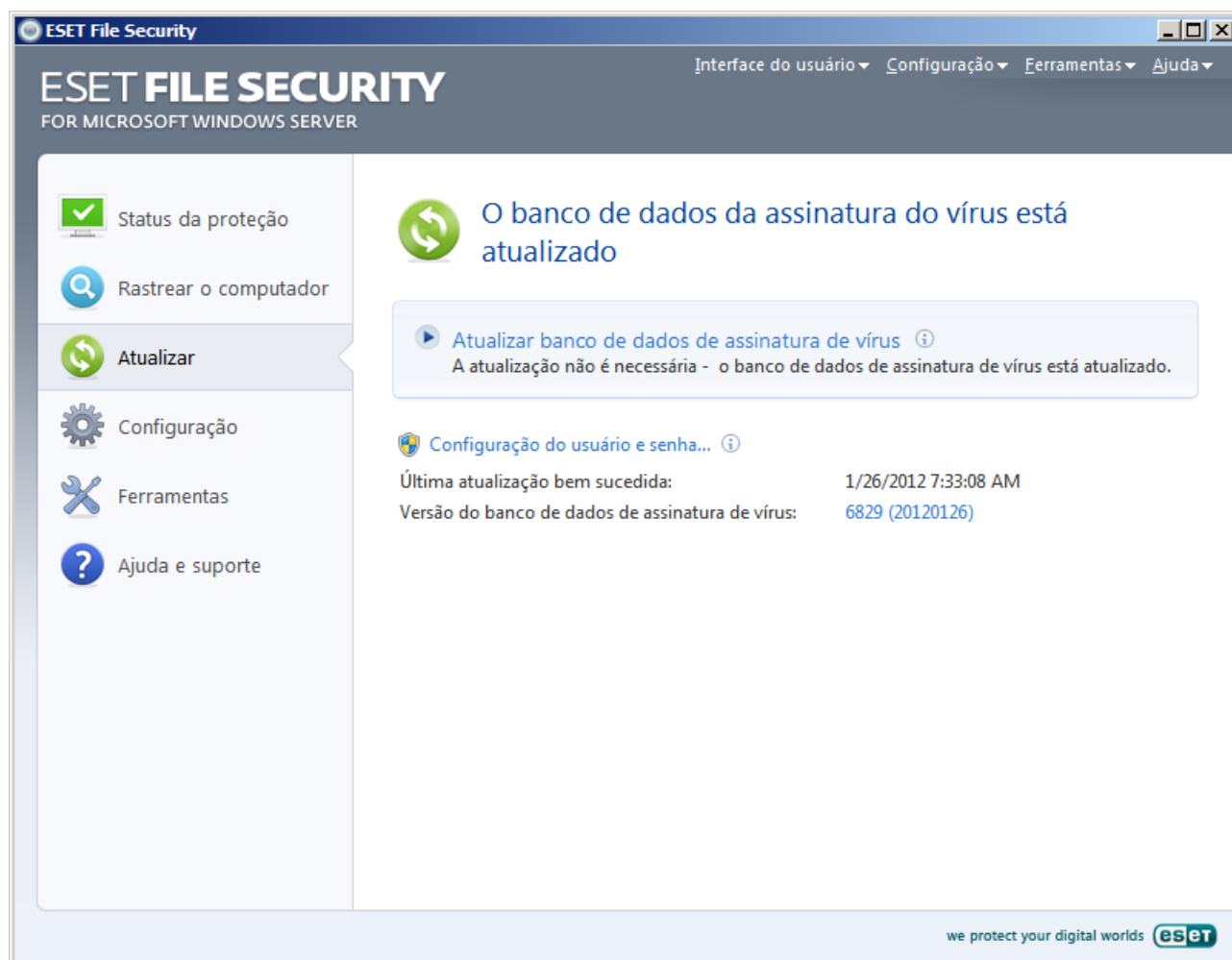
A o clicar no item **Monitorar atividade** do submenu, você poderá monitorar a atividade atual do sistema de arquivos de forma gráfica em tempo real (eixo horizontal). O eixo vertical exibe a quantidade de dados lidos (linha azul) e de dados gravados (linha vermelha).

O submenu **Estatísticas** possibilita ver a quantidade de objetos infectados e limpos de um módulo em particular. Há vários módulos dos quais você pode escolher, selecionando-os na lista suspensa.

3.1.2 O que fazer se o programa não funcionar adequadamente

Se os módulos ativados estiverem funcionando adequadamente, uma marcação verde será atribuída a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido, e informações adicionais sobre o módulo serão mostradas na parte superior da janela. Uma solução sugerida para corrigir o módulo também é exibida. Para alterar o status dos módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.

Se não for possível solucionar um problema com as soluções sugeridas, clique em Ajuda e suporte para acessar os arquivos de ajuda ou pesquisar na base de dados de conhecimento. Se ainda precisar de ajuda, envie uma solicitação de suporte ao Atendimento ao cliente da ESET. O Atendimento ao cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a determinar uma resolução.

3.2 Configuração da atualização

A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são uma parte importante no fornecimento de uma proteção completa contra códigos maliciosos. Dê atenção à sua configuração e operação. No menu principal, selecione **Atualizar** e, em seguida, clique em **Atualizar banco de dados de assinatura de vírus** a primeira janela para verificar se há uma atualização do banco de dados mais recente. **Configuração do usuário e senha...** exibe uma caixa de diálogo em que se deve inserir o nome de usuário e a senha (recebidos após a compra do produto).

Se o nome de usuário e a senha foram inseridos durante a instalação do ESET File Security, essas informações não serão solicitadas aqui.

A janela Configuração avançada (clique em **Configuração** no menu principal e, em seguida, clique em **Entrar na configuração avançada...**, ou pressione F5) contém opções de atualização adicionais. Clique em **Atualizar** na árvore Configuração avançada. O menu suspenso **Atualizar servidor**: deve ser configurado como **Escolher automaticamente**. Para configurar as opções avançadas de atualização, como o modo de atualização, o acesso ao servidor proxy, as conexões de rede e a criação de cópias do banco de dados de assinatura de vírus, clique no botão **Configuração...**.

ESET File Security

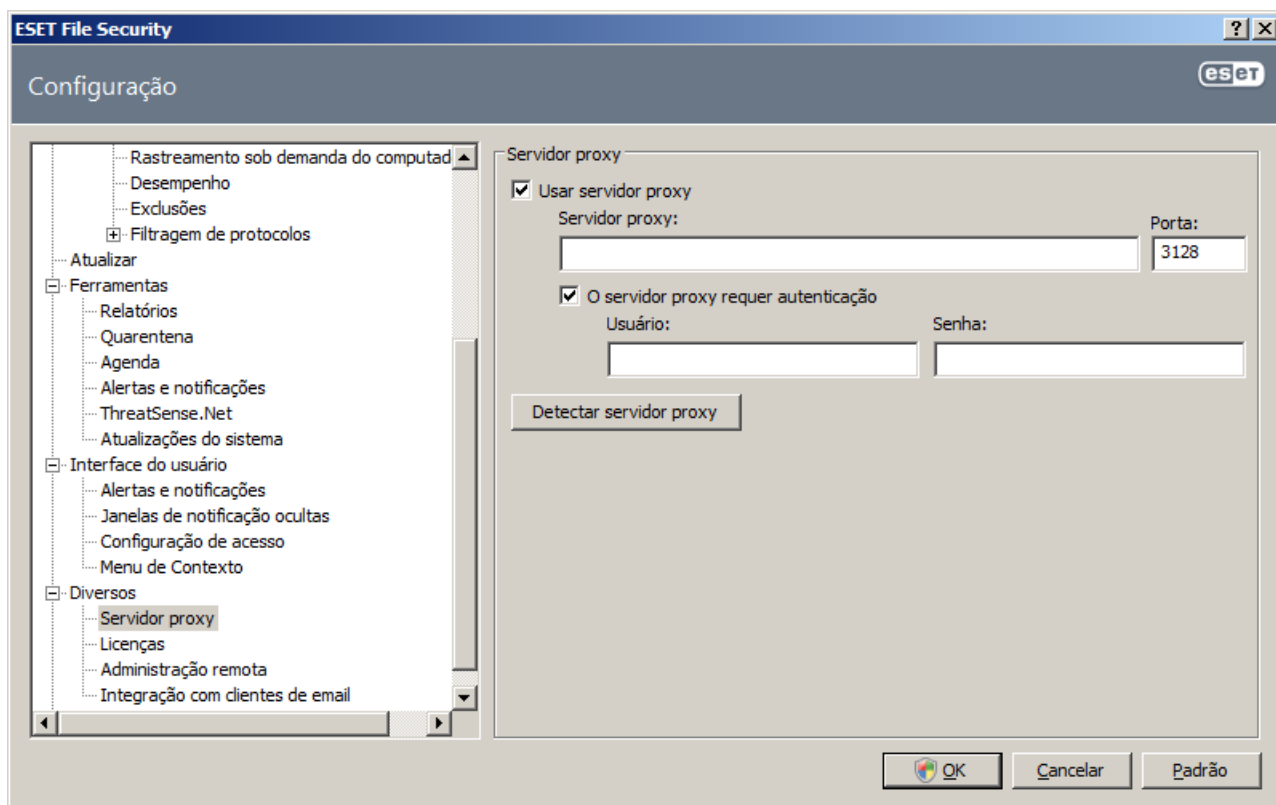
Configuração

Proteção do servidor
Exclusões automáticas
Proteção do computador
Antivírus e antispyware
Proteção em tempo real do sistema de arc
Configuração avançada
Proteção de documentos
Proteção do cliente de email
POP3, POP3s
Proteção do acesso à Web
HTTP, HTTPs
Rastreamento sob demanda do computad
Desempenho
Exclusões
Filtragem de protocolos
Atualizar
Ferramentas
Relatórios
Quarentena
Agenda
Alertas e notificações
ThreatSense.Net

Perfil selecionado:
Meu perfil
Perfis...
Atualizar configurações do perfil selecionado
Servidor de Atualização:
Escolher automaticamente
Editar...
Usuário:
lupdv4
Senha:
••••••••••
Configuração avançada de atualização:
Configurar...
Limpar cache de atualização:
Limpar
Não exibir notificação sobre atualização bem-sucedida

OK
Cancelar
Padrão

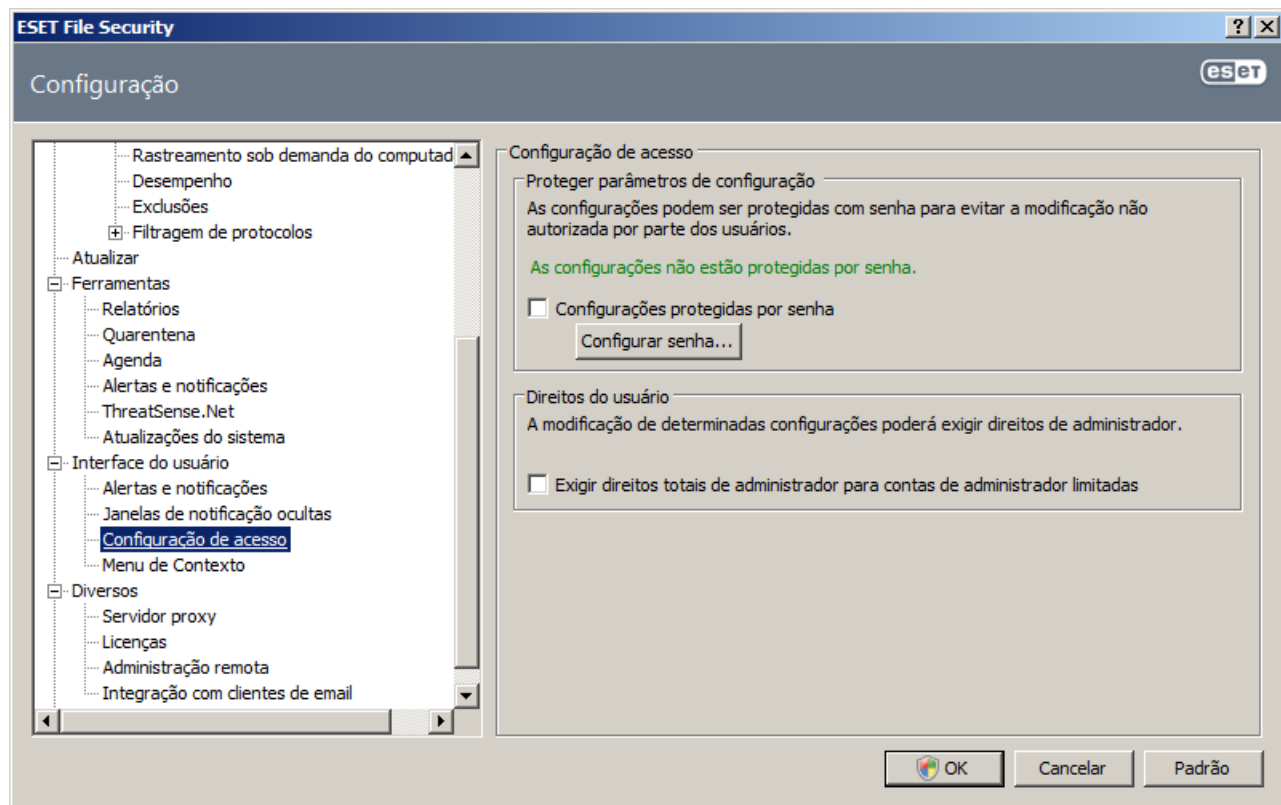
3.3 Configuração do servidor proxy

Se estiver usando um servidor proxy para controlar as conexões à Internet em um sistema que usa o ESET File Security, isso deve ser especificado nas Configurações avançadas. Para acessar a janela de configuração do servidor proxy, pressione F5 para abrir a janela Configurações avançadas e clique em **Diversos** > **Servidor proxy** na árvore Configurações avançadas. Selecione a opção **Utilizar servidor proxy** e, em seguida, preencha os campos **Servidor proxy** (Endereço IP) e **Porta**. Se necessário, selecione a opção **O servidor proxy requer autenticação** e digite um **Nome de usuário** e uma **Senha**.

Se estas informações não estiverem disponíveis, tente detectar automaticamente as configurações de servidor proxy clicando no botão **Detectar servidor proxy**.

OBSERVAÇÃO: As opções de servidor proxy para diferentes perfis de atualização podem variar. Se este for o caso, configure diferentes perfis de atualização em Configurações avançadas clicando em **Atualizar** na árvore Configurações avançadas.

3.4 Proteção de configurações

As configurações do ESET File Security podem ser muito importantes da perspectiva da política de segurança da organização. Modificações não autorizadas podem pôr potencialmente em risco a estabilidade e a proteção do seu sistema. Para proteger por senha os parâmetros de configuração, no menu principal clique em **Configuração** > **Entrar na configuração avançada...** > **Interface do usuário** > **Configuração de acesso**, selecione a opção **Configurações protegidas por senha** e clique no botão **Configurar senha...**.

Digite uma senha nos campos **Nova senha** e **Confirmar nova senha** e clique em **OK**. Esta senha será necessária no futuro sempre que forem feitas alterações ao ESET File Security.

OBSERVAÇÃO: Clique aqui para ver como configurar isto pelo eShell

4. Trabalho com o ESET File Security

4.1 ESET File Security - Proteção do servidor

O ESET File Security oferece proteção para seu servidor com recursos essenciais, como: Antivírus e Antispyware, Proteção residente (Proteção em tempo real), proteção do acesso à Web e Proteção do cliente de email. Você pode ler mais sobre cada tipo de proteção na seção ESET File Security - Proteção do computador. Além disso, há um recurso chamado Exclusões automáticas. Ele identifica aplicativos críticos de servidor e arquivos do sistema operacional do servidor e os adiciona automaticamente à lista de Exclusões. Essa funcionalidade reduzirá o risco de possíveis conflitos e aumenta o desempenho geral do servidor ao executar o software antivírus.

4.1.1 Exclusões automáticas

Os desenvolvedores de aplicativos de servidor e sistemas operacionais recomendam excluir conjuntos de arquivos e pastas críticos de trabalho do rastreamento do antivírus para a maioria de seus produtos. Os rastreamentos de antivírus podem ter uma influência negativa no desempenho de um servidor, levar a conflitos e até impedir que alguns aplicativos sejam executados no servidor. As exclusões ajudam a reduzir o risco de possíveis conflitos e aumentam o desempenho geral do servidor ao executar o software antivírus.

O ESET File Security identifica aplicativos críticos de servidor e arquivos do sistema operacional do servidor e os adiciona automaticamente à lista de Exclusões. Após a adição, o processo/aplicativo do servidor pode ser ativado (por padrão) marcando-se a opção apropriada, ou desativado desmarcando-a, com o seguinte resultado:

1) Se uma exclusão de aplicativo/sistema operacional permanecer ativada, qualquer de seus arquivos e pastas críticos será adicionado à lista de arquivos excluídos do rastreamento (**Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões**). Sempre que o servidor for reiniciado, o sistema realiza uma verificação automática das exclusões e restaura quaisquer exclusões que possam ter sido excluídas da lista. Esta é a configuração recomendada se quiser garantir que as Exclusões automáticas recomendadas sejam sempre aplicadas.

2) Se um usuário desativar uma exclusão de aplicativo/sistema operacional, seus arquivos e pastas críticos permanecerão na lista de arquivos excluídos do rastreamento (**Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões**). No entanto, eles não serão verificados ou renovados automaticamente na lista **Exclusões** sempre que o servidor for reiniciado (veja o ponto 1 acima). Recomendamos esta configuração para usuários avançados, que desejam remover ou alterar algumas exclusões padrão. Se quiser remover as exclusões da lista sem reiniciar o servidor, você precisará removê-las manualmente da lista (**Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões)**.

Nenhuma exclusão definida pelo usuário e inserida manualmente em **Configuração avançada** > **Proteção do computador** > **Antivírus e antispyware** > **Exclusões** será afetada pelas configurações descritas anteriormente.

As Exclusões automáticas de aplicativos/sistemas operacionais do servidor são selecionadas com base nas recomendações da Microsoft. Para obter detalhes, consulte os seguintes links:

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

4.2 ESET File Security - Proteção do computador

O ESET File Security tem todas as ferramentas necessárias para garantir a proteção do servidor como um computador. Ele oferece proteção significativa para seu servidor, com os seguintes tipos de proteção: Antivírus e Antispyware, Proteção residente (Proteção em tempo real), proteção do acesso à Web e Proteção do cliente de email.

4.2.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, e-mails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la primeiro bloqueando-a e em seguida, limpando, excluindo ou movendo-a para a quarentena.

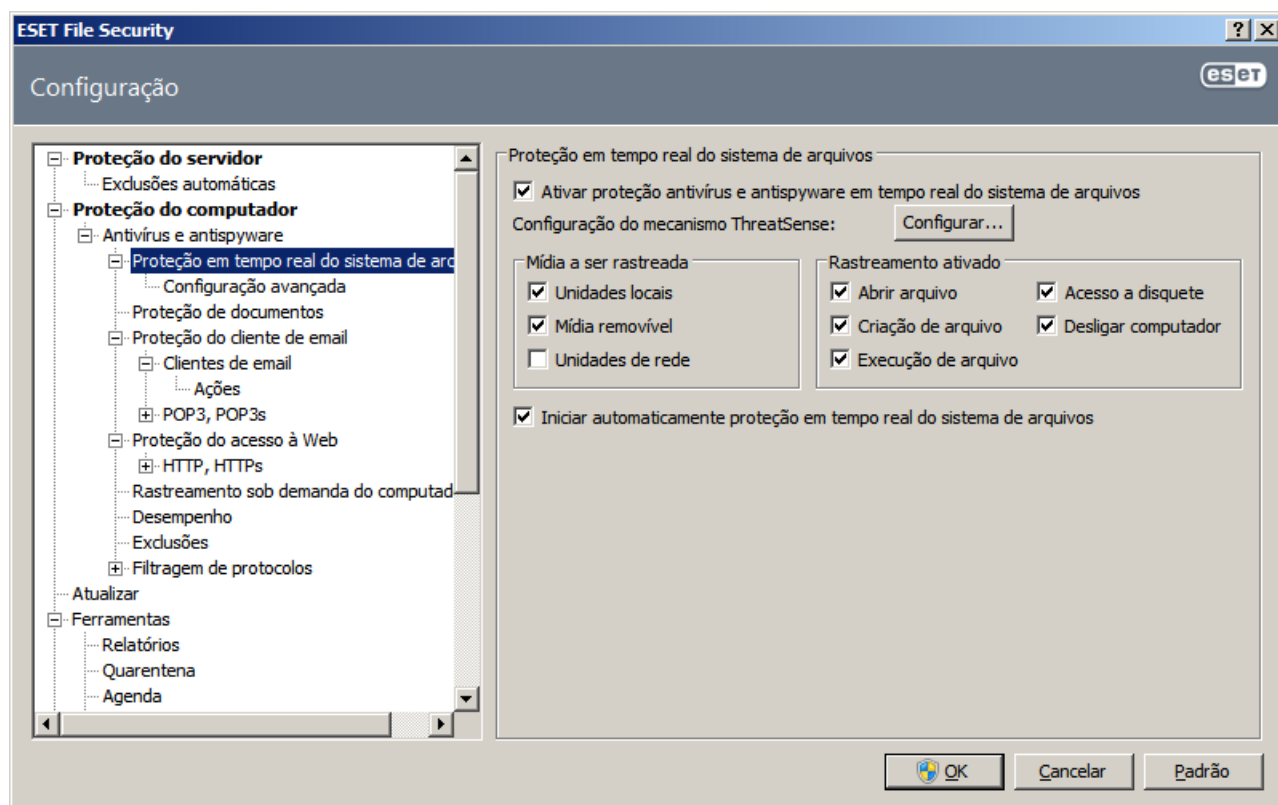
4.2.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.

4.2.1.1.1 Configuração de controle

A proteção do sistema de arquivos em tempo real verifica todos os tipos de mídia e é acionada por vários eventos. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo ThreatSense), a proteção do sistema de arquivos em tempo real pode variar para arquivos recém-criados e existentes. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

Para proporcionar o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é configurado usando a Otimização inteligente. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Para modificar essa opção, abra a janela Configuração avançada e clique em **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Depois, clique no botão **Configuração...** ao lado de **Configuração do mecanismo ThreatSense**, clique em **Outros** e marque ou desmarque a opção **Ativar otimização inteligente**.

Por padrão, a proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver conflito com outro scanner em tempo real), a proteção em tempo real pode ser encerrada, desmarcando a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos**.

4.2.1.1.1.1 Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças.

Unidades locais – Controla todas as unidades de disco rígido do sistema

Mídia removível – Disquetes, dispositivos de armazenamento USB, etc.

Unidades de rede – Rastreia todas as unidades mapeadas

Recomendamos manter as configurações padrão e modificá-las somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

4.2.1.1.1.2 Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

A opção **Acesso a disquete** proporciona controle do setor de inicialização do disquete quando essa unidade for acessada. A opção **Desligar computador** proporciona controle dos setores de inicialização do disco rígido durante o desligamento do computador. Embora os vírus de inicialização sejam raros atualmente, recomendamos deixar essas opções ativadas, pois sempre há a possibilidade de infecção por um vírus de inicialização de origem alternativa.

4.2.1.1.1.3 Opções de rastreamento avançadas

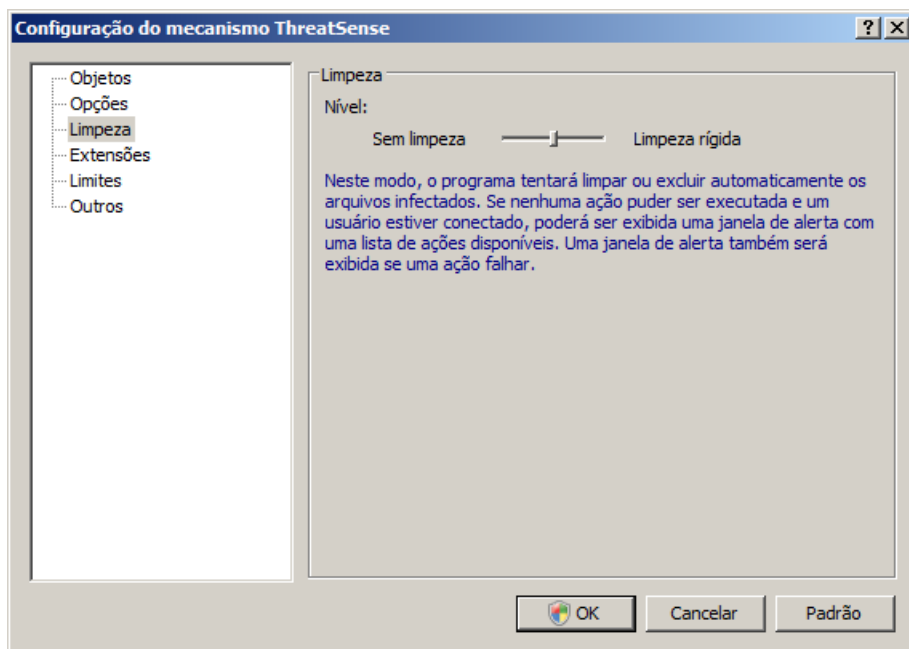
Opções de configuração mais detalhadas podem ser encontradas em **Proteção do computador** > **Antivírus e antispyware** > **Proteção em tempo real do sistema** > **Configuração avançada**.

Parâmetros adicionais do ThreatSense para arquivos criados e modificados recentemente – A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior que em arquivos existentes. É por isso que o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, é usada a heurística avançada, que aumenta enormemente os índices de detecção. Além dos arquivos recém-criados, o rastreamento também é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo de real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desmarque a opção Configurações padrão de rastreamento em arquivos compactados.

Parâmetros ThreatSense.Net adicionais para arquivos executados – Por padrão, a heurística avançada não é usada quando os arquivos são executados. Entretanto, em alguns casos pode ser necessário ativar essa opção (marcando a opção **Heurística avançada na execução de arquivos**). Observe que a heurística avançada pode tornar mais lenta a execução de alguns programas devido ao aumento dos requisitos do sistema.

4.2.1.1.2 Níveis de limpeza

A proteção em tempo real têm três níveis de limpeza. Para selecionar um nível de limpeza, clique no botão **Configuração...** na seção **Proteção em tempo real do sistema de arquivos** e clique na ramificação **Limpeza**.

- O primeiro nível, **Sem limpeza**, exibe uma janela de alerta com as opções disponíveis para cada ameaça encontrada. É necessário escolher uma ação para cada infiltração individualmente. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.
- O nível padrão escolhe e executa automaticamente uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma mensagem localizada no canto inferior direito da tela. As ações automáticas não são realizadas quando a infiltração estiver localizada dentro de um arquivo compactado (que também contém arquivos limpos) ou quando os objetos infectados não tiverem uma ação predefinida.
- O terceiro nível, **Limpeza rígida**, é o mais “agressivo” – todos os objetos infectados são limpos. Uma vez que esse nível poderia potencialmente resultar em perda de arquivos válidos, recomendamos que seja usado somente em situações específicas.

4.2.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Portanto, seja cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver conflito com um certo aplicativo ou scanner em tempo real de outro programa antivírus.

Após a instalação do ESET File Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior direita da janela **Proteção em tempo real do sistema de arquivos** (**Configuração avançada** > **Antivírus e antispyware** > **Proteção em tempo real do sistema de arquivos**).

4.2.1.1.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.org. Esse arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo eicar.com está disponível para download em http://www.eicar.org/download/eicar.com

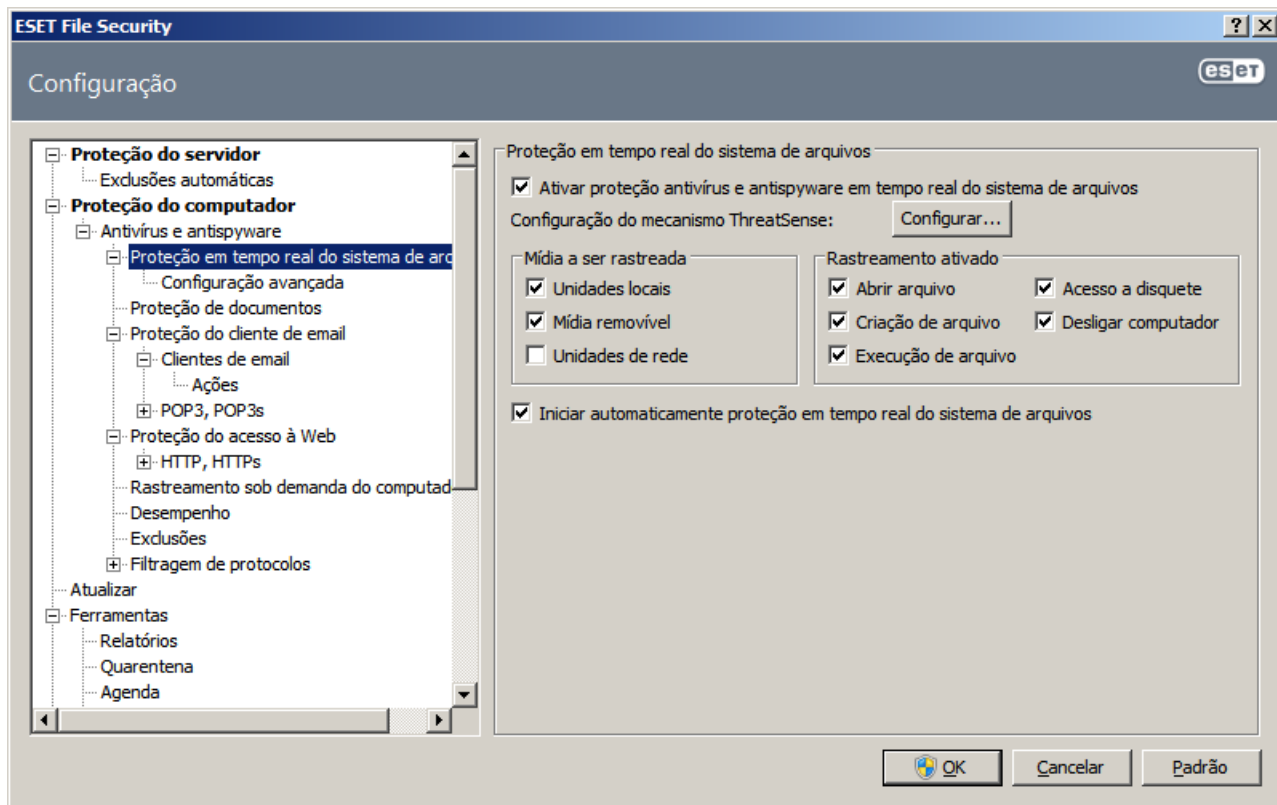
OBSERVAÇÃO: Antes de executar uma verificação da proteção em tempo real, é necessário desativar o firewall. Se o firewall estiver ativado, ele detectará e impedirá o download do arquivo de teste.

4.2.1.1.5 O que fazer se a proteção em tempo real não funcionar

No próximo capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

A proteção em tempo real está desabilitada

Se a proteção em tempo real tiver sido inadvertidamente desativada por um usuário, será preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** > **Antivírus e antispyware** e clique na seção **Ativar a proteção em tempo real do sistema de arquivos** da janela principal do programa.

Se a proteção em tempo real não for ativada na inicialização do sistema, isso provavelmente será devido à não ativação da opção **Inicialização automática da proteção em tempo real no sistema de arquivos**. Para ativar essa opção, navegue até Configuração avançada (F5) e clique em **Proteção em tempo real do sistema de arquivos** na árvore Configuração avançada. Na seção **Configuração avançada** na parte inferior da janela, certifique-se de que a caixa de seleção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está selecionada.

Se a proteção em tempo real não detectar nem limpar infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** estiver ativada), isso pode ser devido a conflitos com outros programas. Se for este o caso, consulte os especialistas do Serviço ao Cliente da ESET.

4.2.1.2 Proteção de cliente de email

A proteção de e-mail fornece controle da comunicação por e-mail recebida via protocolo POP3. Usando o plug-in para Microsoft Outlook, o ESET File Security permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP).

Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado oferecidos pelo mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com o banco de dados de assinaturas de vírus. O rastreamento das comunicações via protocolo POP3 é independente do cliente de email usado.

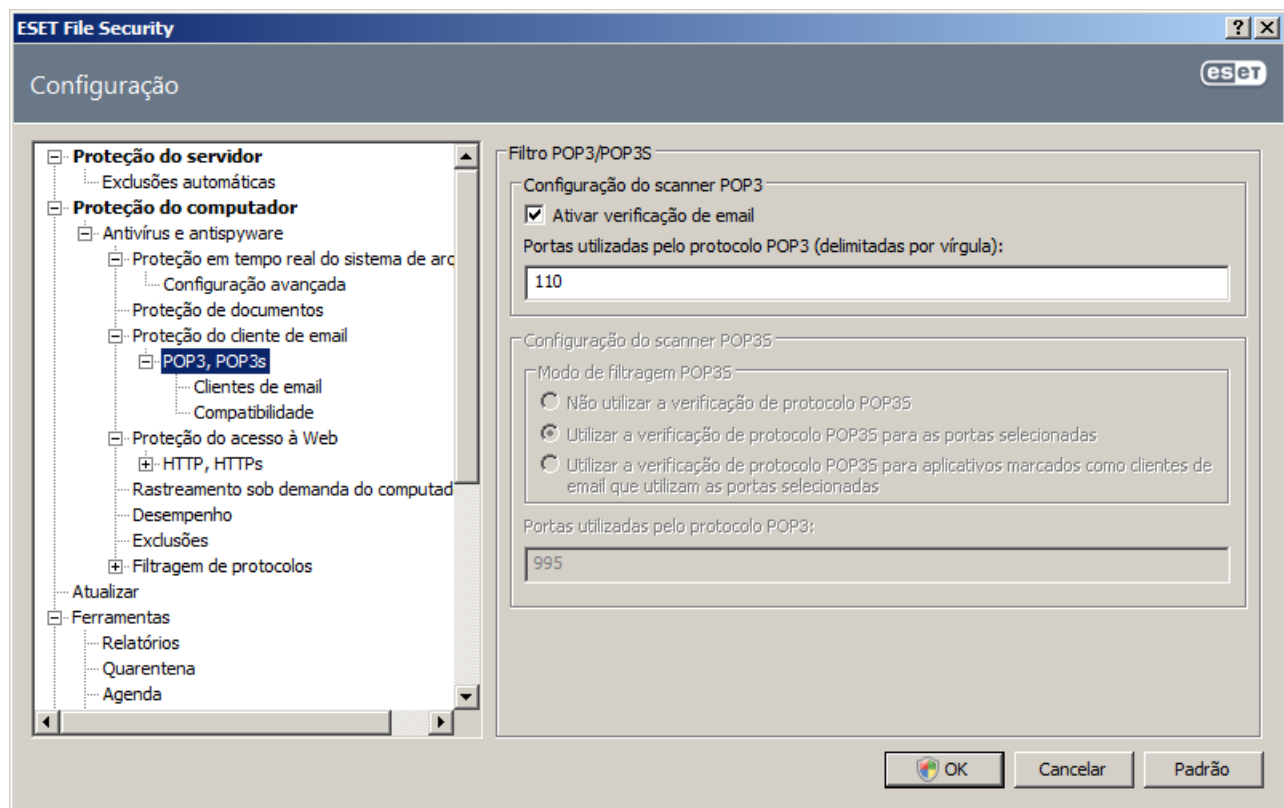
4.2.1.2.1 Rastreamento POP3

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET File Security fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado – a verificação do POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

A comunicação criptografada não é controlada.

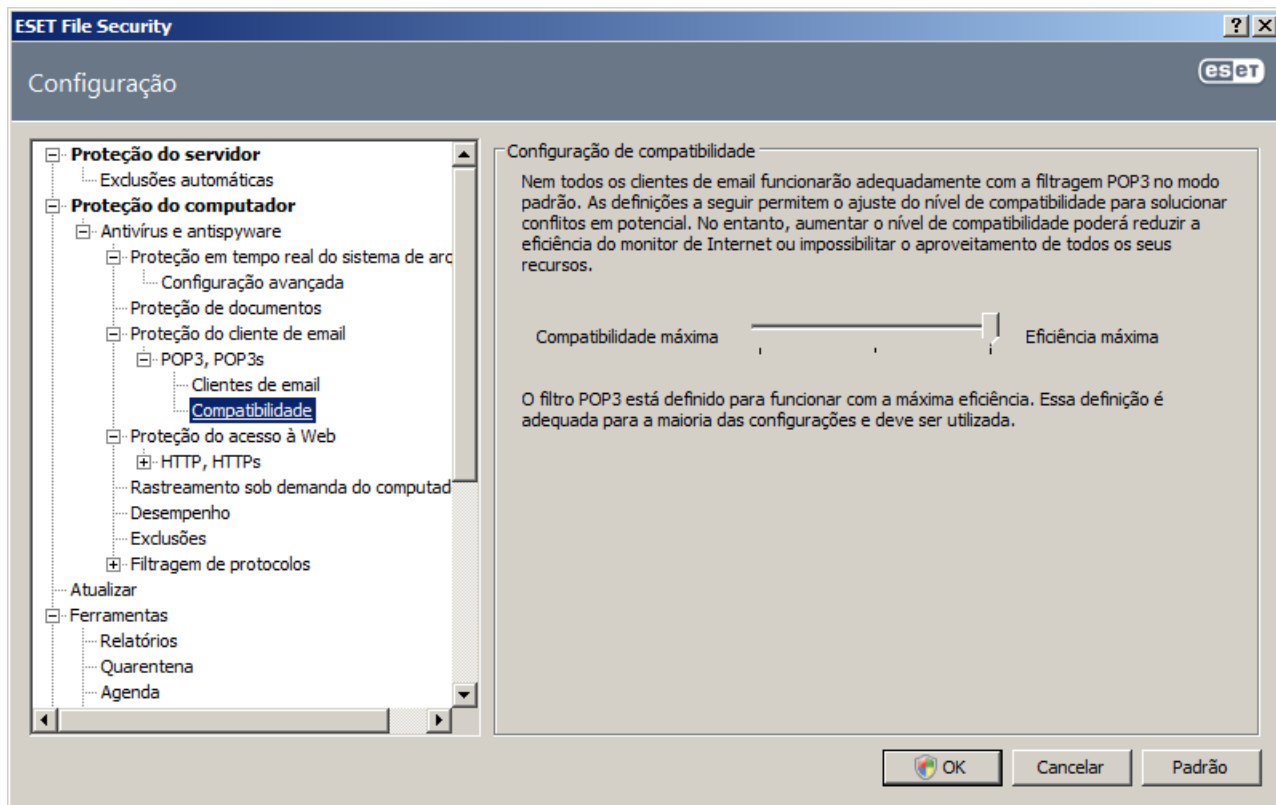
Para poder usar a filtragem de POP3/POP3S, é necessário ativar primeiro a Filtragem de protocolos. Se as opções de POP3/POP3S estiverem acinzentadas, navegue até **Proteção do computador** > **Antivírus e antispyware** > **Filtragem de protocolos** na árvore de configuração avançada e selecione **Ativar filtragem de conteúdo do**

protocolo de aplicativo. Consulte a seção Filtragem de protocolos para obter mais detalhes sobre filtragem e configuração.

4.2.1.2.1.1 Compatibilidade

Determinados programas de email podem ter problemas com a filtragem POP3 (por exemplo, ao receber mensagens com uma conexão lenta de Internet, poderá ocorrer desativação por ultrapassar o limite de tempo devido à verificação). Se for este o caso, tente modificar a maneira como é feito o controle. A redução do nível de controle pode melhorar a velocidade do processo de limpeza. Para ajustar o nível de controle da filtragem POP3, na árvore Configuração avançada, navegue até **Antivírus e antispyware** > **Proteção de email** > **POP3, POP3s** > **Compatibilidade**.

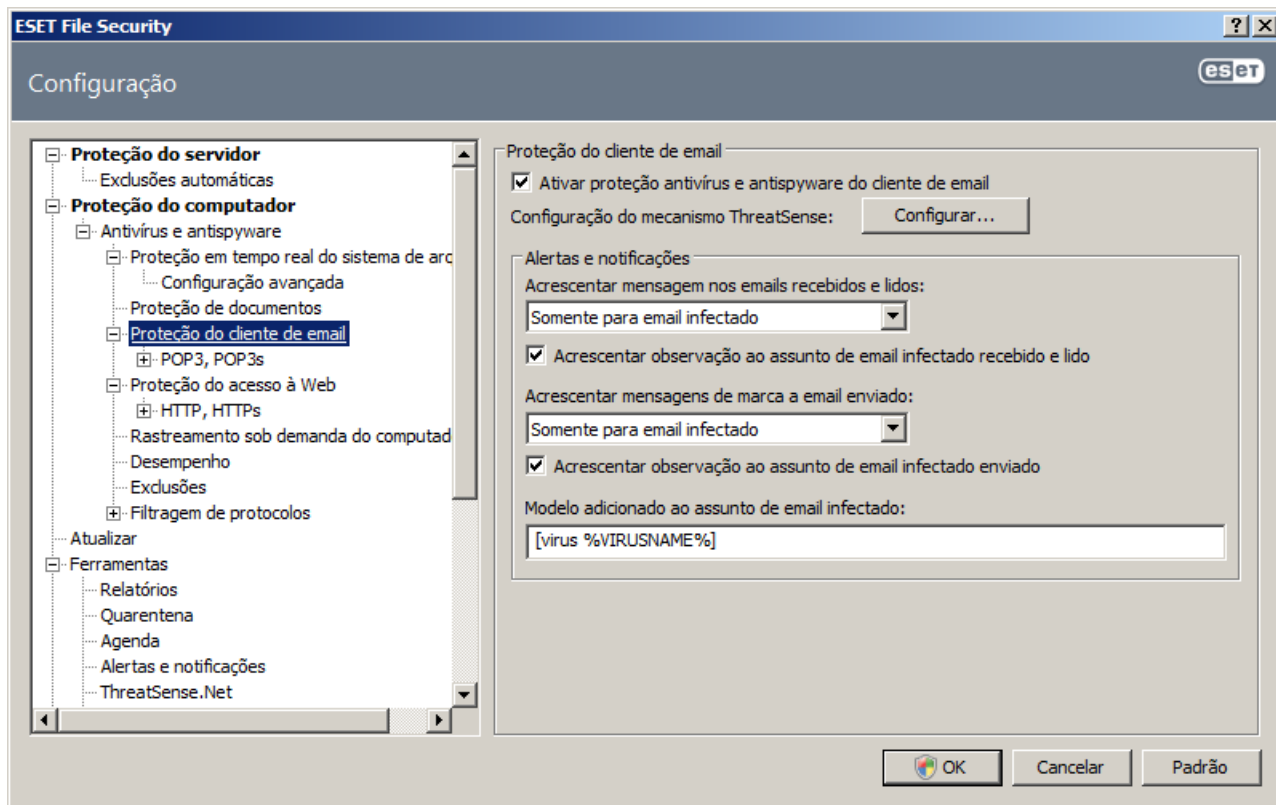
Se for ativada a **Eficiência máxima**, as infiltrações serão removidas das mensagens infectadas e as informações sobre a infiltração serão inseridas na frente do assunto original do email (as opções **Excluir** ou **Limpar** devem estar ativadas ou o nível de limpeza **Rígida** ou **Padrão** deve estar ativado).

Compatibilidade média modifica a maneira como as mensagens são recebidas. As mensagens serão gradualmente enviadas ao cliente de email. Após a mensagem ser transferida, ela será rastreada quanto a infiltrações. O risco de infecção aumenta com esse nível de controle. O nível de limpeza e o processamento de mensagens de marca (alertas de notificação anexos à linha do assunto e corpo dos emails) são idênticos à configuração de eficiência máxima.

Com o nível de **Compatibilidade máxima**, você será avisado por uma janela de alerta, que informará o recebimento de uma mensagem infectada. Não é adicionada nenhuma informação sobre arquivos infectados à linha do assunto ou ao corpo do email de mensagens entregues e as infiltrações não são automaticamente removidas; é necessário excluir as infiltrações do cliente de email.

4.2.1.2.2 Integração com clientes de email

A integração do ESET File Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET File Security. Se a integração for ativada, a barra de ferramentas do ESET File Security será inserida diretamente no cliente de email, permitindo proteção mais eficiente aos emails. As configurações de integração estão disponíveis em **Configuração** > **Entrar na configuração avançada...** > **Diversos** > **Integração com clientes de email**. A integração com clientes de email permite ativar a integração com os clientes de email compatíveis. Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

Selecione a opção **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email. Essa situação pode ocorrer ao fazer download de email do Kerio Outlook Connector Store

A proteção de email é ativada clicando em **Configuração** >**Entrar na configuração avançada...** > **Antivírus e antispyware** > **Proteção do cliente de email** e selecionando a opção **Ativar proteção antivírus e antispyware do cliente de email**.

4.2.1.2.2.1 Anexar mensagens de marca ao corpo de um email

Todo email rastreado pelo ESET File Security pode ser marcado anexando uma mensagem de marca ao assunto ou ao corpo do e-mail. Esse recurso aumenta o nível de credibilidade para os destinatários e se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** > **Antivírus e antispyware** > **Proteção do cliente de email**. É possível selecionar **Acrescentar mensagem nos emails recebidos e lidos**, bem como **Acrescentar mensagens de marca a email enviado**. Também há a possibilidade de anexar mensagens de marca a todos os emails rastreados, a somente emails infectados ou a nenhum.

O ESET File Security também permite anexar mensagens ao assunto original de mensagens infectadas. Para permitir a anexação ao assunto, selecione as opções **Acrescentar observação ao assunto de email infectado recebido e lido** e **Acrescentar observação ao assunto de email infectado enviado**.

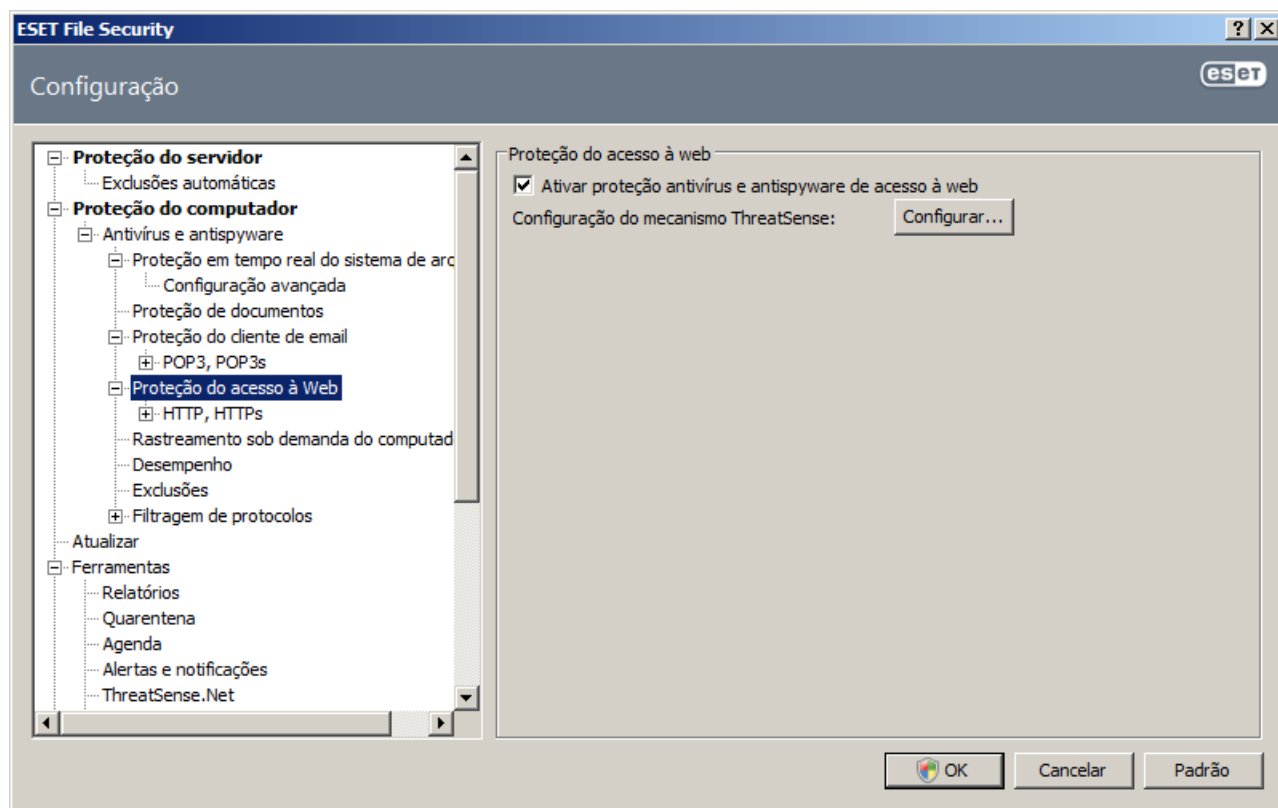
O conteúdo das notificações pode ser modificado no campo **Modelo adicionado ao assunto de email infectado**. As modificações mencionadas anteriormente podem ajudar a automatizar o processo de filtragem dos emails infectados, pois permite filtrar emails com um assunto específico (se houver suporte no cliente de email) em uma pasta separada.

4.2.1.2.3 Removendo infiltrações

Se uma mensagem de email infectada for recebida, uma janela de alerta será exibida. A janela de alerta mostra o nome do remetente, o email e o nome da infiltração. Na parte inferior da janela, as opções **Limpar**, **Excluir** ou **Deixar** estarão disponíveis para cada objeto detectado. Na maioria dos casos, recomendamos selecionar **Limpar** ou **Excluir**. Em determinadas situações, se desejar receber o arquivo infectado, selecione **Deixar**.

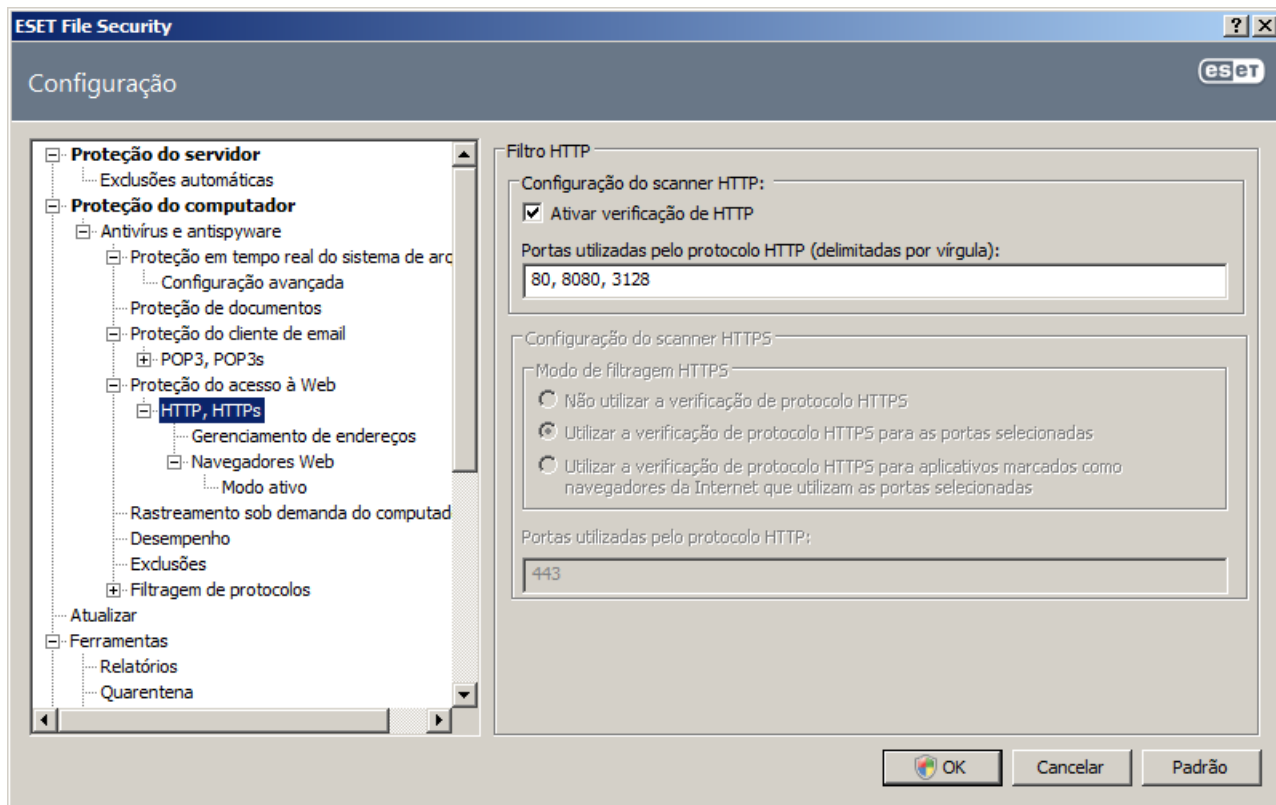
Se a **Limpeza rígida** estiver ativada, uma janela de informações sem nenhuma opção disponível para os objetos infectados será exibida.

4.2.1.3 Proteção do acesso à web

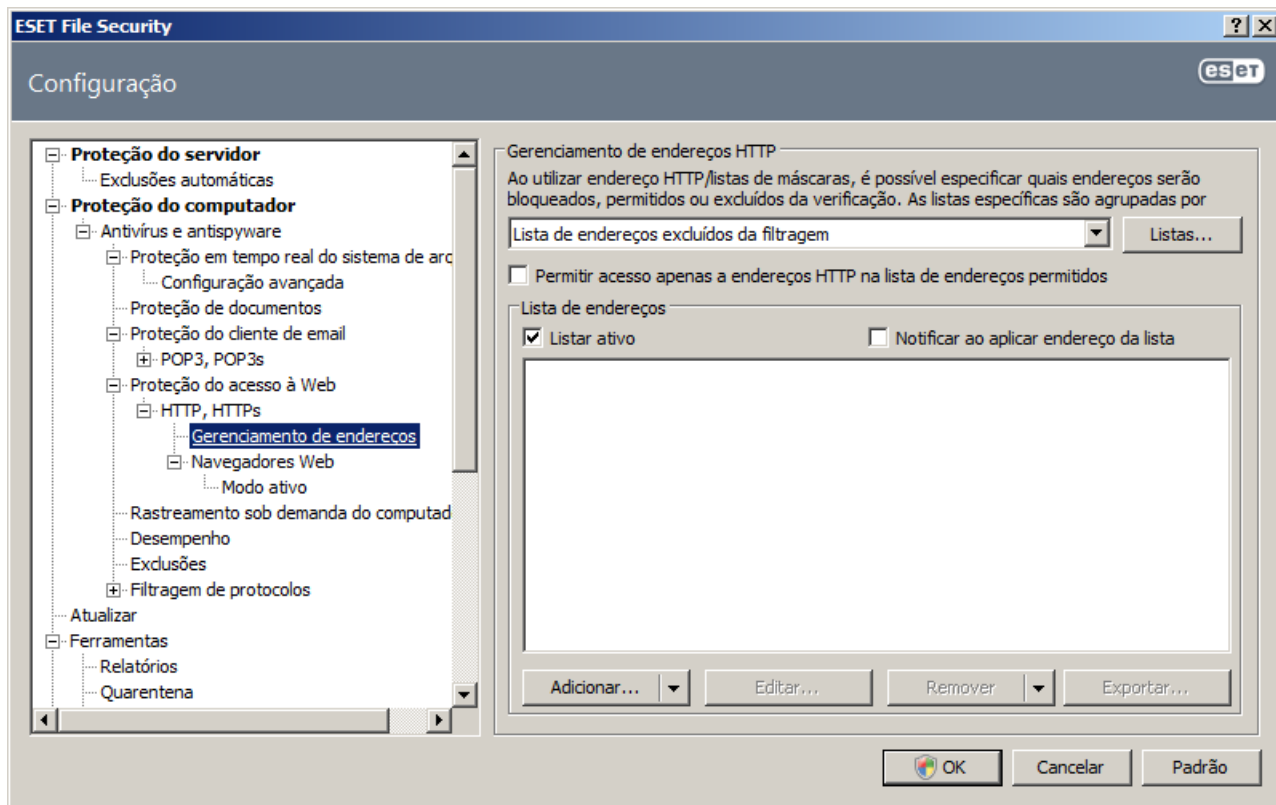
A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. Por isso, é essencial refletir com atenção sobre a proteção do acesso à Web. Recomendamos enfaticamente que a opção **Ativar proteção antivírus e antispyware de acesso à web** seja selecionada. Essa opção está localizada em **Configuração** (F5) > **Antivírus e antispyware** > **Proteção do acesso à web**.

4.2.1.3.1 HTTP, HTTPs

A proteção de acesso à Web funciona monitorando a comunicação entre os navegadores da Internet e servidores remotos e cumprem as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPs (comunicação criptografada). Por padrão, o ESET File Security está configurado para usar os padrões da maioria dos navegadores de Internet. Contudo, as opções de configuração do scanner HTTP podem ser modificadas em **Configuração avançada** (F5) > **Antivírus e antispyware** > **Proteção do acesso à web** > **HTTP, HTTPS**. Na janela principal do filtro HTTP, é possível selecionar ou desmarcar a opção **Ativar verificação de HTTP**. Você também pode definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80, 8080 e 3128 estão predefinidos. A verificação de HTTPs pode ser executada nos seguintes modos:

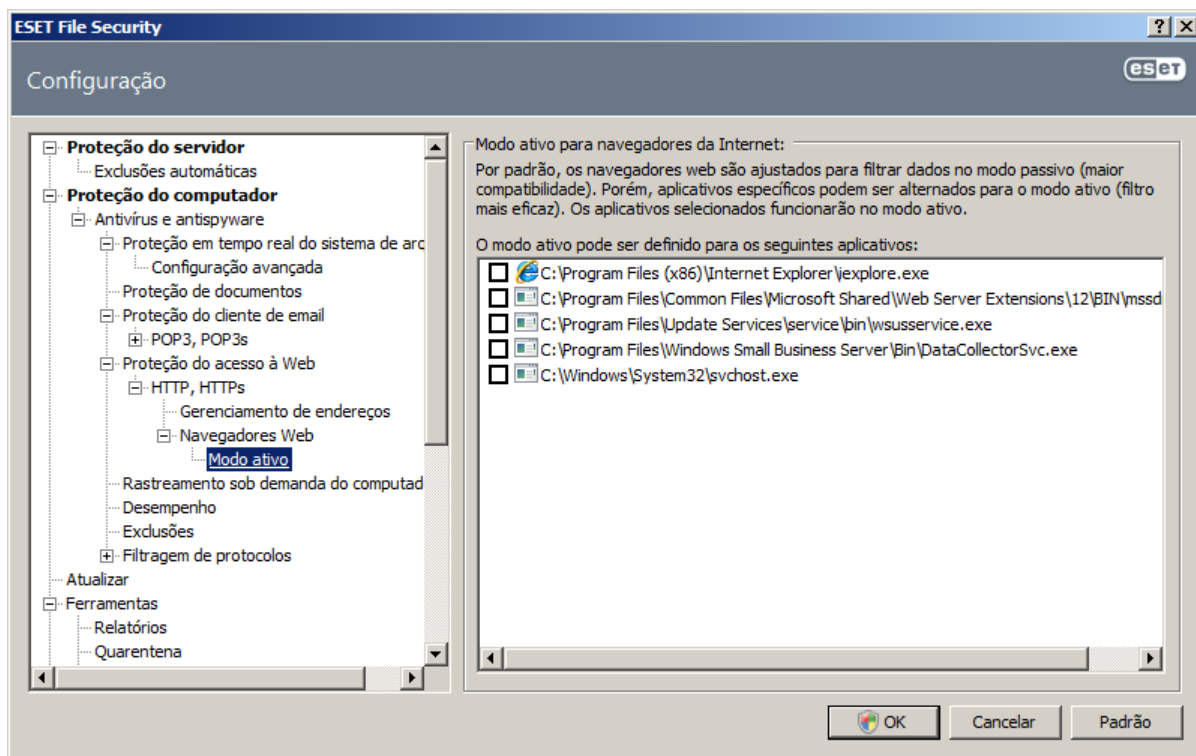
Não utilizar a verificação de protocolo HTTPS – A comunicação criptografada não será verificada

Utilizar a verificação de protocolo HTTPS para as portas selecionadas – Verificação de HTTPs apenas para as portas definidas em **Portas usadas pelo protocolo HTTPs**

4.2.1.3.1.1 Gerenciamento de endereços

Essa seção permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação. Os botões **Adicionar...**,**Editar...**, **Remover** e **Exportar...** são utilizados para gerenciar as listas de endereços. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso. Se você selecionar a opção **Permitir acesso apenas a endereços HTTP na lista de endereços permitidos**, apenas endereços presentes na lista de endereços permitidos serão acessíveis, enquanto todos os outros endereços HTTP serão bloqueados.

Em todas as listas, os símbolos especiais * (asterisco) e? (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Para ativar uma lista, selecione a opção **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione a opção **Notificar ao aplicar endereço da lista**.

4.2.1.3.1.2 Modo ativo

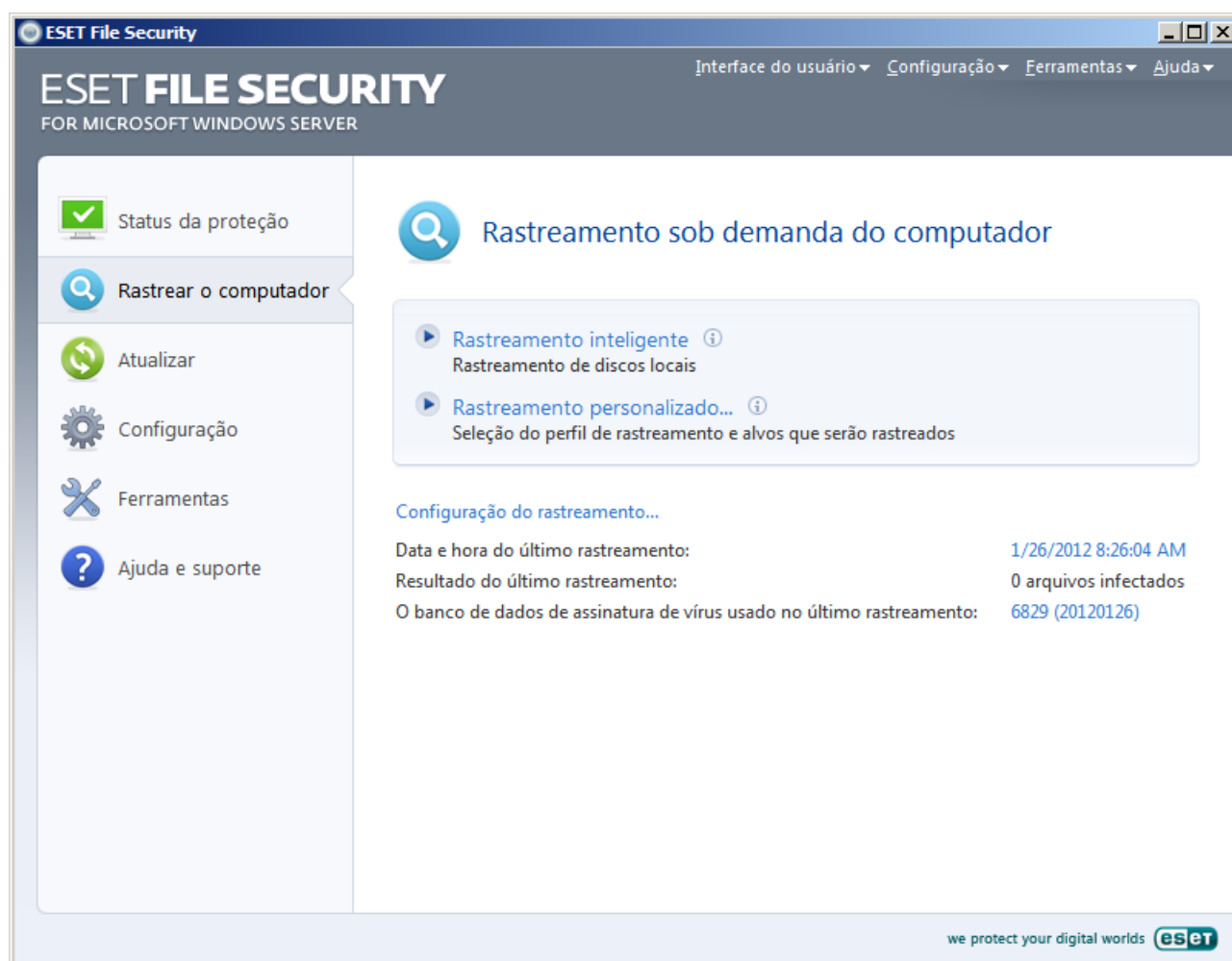
A lista dos aplicativos marcados como navegadores da Web pode ser acessada diretamente no submenu **Navegadores web** da ramificação **HTTP, HTTPs**. Esta seção também contém o submenu **Modo Ativo**, que define o modo de verificação para os navegadores da Internet.

O **Modo ativo** é útil porque examina os dados transferidos como um todo. Se não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também fornece maior compatibilidade para os aplicativos listados. Se nenhum problema ocorrer durante ao usá-lo, recomendamos que você ative o modo de verificação ativo marcando a caixa de seleção ao lado do aplicativo desejado.

4.2.1.4 Rastreamento sob demanda do computador

Caso suspeite que seu computador está infectado (se ele se comportar de maneira anormal), execute um rastreamento sob demanda para examinar se há ameaças no computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. O rastreamento normal pode detectar infiltrações que não foram detectadas pelo scanner em tempo real quando foram salvas no disco. Isso pode acontecer caso o scanner em tempo real esteja desativado no momento da infecção ou se o banco de dados de assinatura de vírus não estiver atualizado.

Recomendamos que execute um Rastreamento sob demanda do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

4.2.1.4.1 Tipos de rastreamento

Há dois tipos de rastreamento sob demanda do computador disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado...** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

4.2.1.4.1.1 Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. Suas principais vantagens são a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a seção Limpeza.

4.2.1.4.1.2 Rastreamento personalizado

O rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de rastreamento, selecione **Rastreamento do computador** > **Rastreamento personalizado** e selecione uma opção no menu suspenso **Alvos de rastreamento** ou selecione alvos específicos na estrutura em árvore. Um alvo de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione a opção **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Limpeza**.

4.2.1.4.2 Alvos de rastreamento

O menu suspenso Alvos de rastreamento permite selecionar arquivos, pastas e dispositivos (discos) que serão rastreados em busca de vírus.

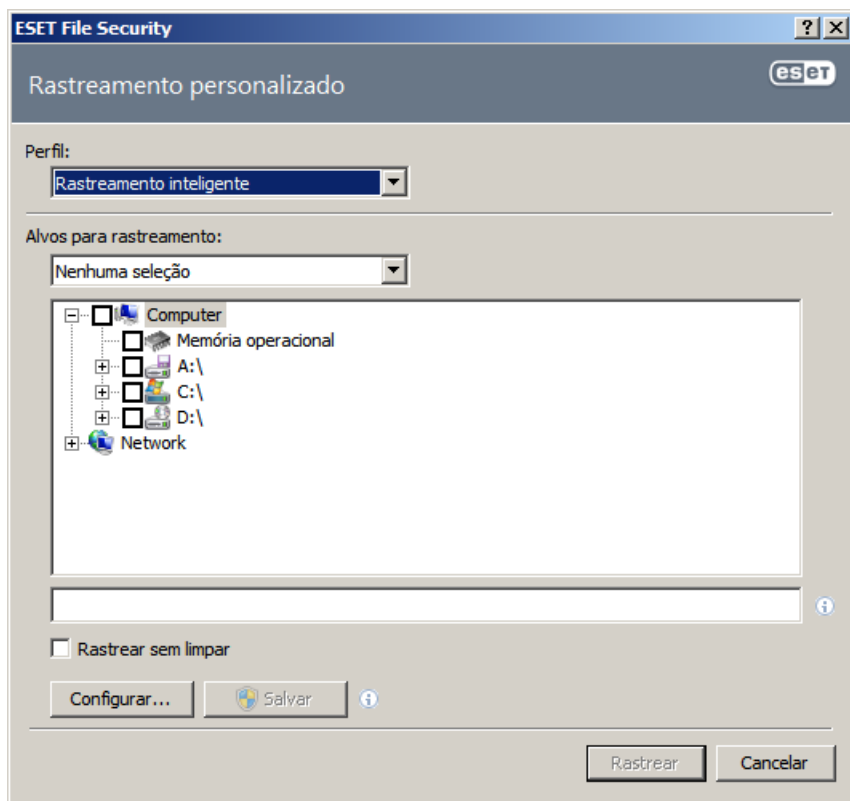
Por configurações de perfil – Seleciona alvos definidos no perfil de rastreamento selecionado

Mídia removível – Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD

Unidades locais – Seleciona todas as unidades de disco rígido do sistema

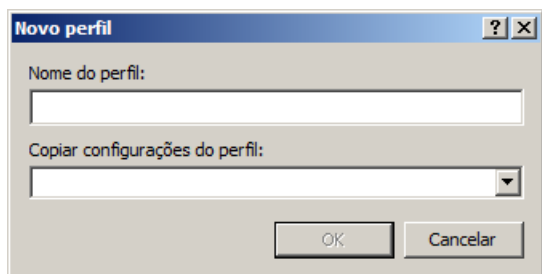
Unidades de rede – Seleciona todas as unidades mapeadas

Nenhuma seleção – Cancela todas as seleções

Um alvo de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador.

4.2.1.4.3 Perfis de rastreamento

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Rastreamento sob demanda do computador** > **Perfis...** A janela **Perfis de configuração** tem um menu suspenso com os perfis de rastreamento existentes, bem como a opção para criar um novo. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

EXEMPLO: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...**. Digite o nome do novo perfil no campo **Nome do perfil** e selecione **Rastreamento inteligente** no menu suspenso **Copiar configurações do perfil**: Depois, ajuste os demais parâmetros de maneira a atender as suas necessidades.

4.2.1.4.4 Linha de comando

O módulo antivírus do ESET File Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat").

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

Opções gerais:

- help	mostrar ajuda e sair
- version	mostrar informações de versão e sair
- base-dir = FOLDER	carregar módulos da PASTA
- quar-dir = FOLDER	PASTA de quarentena
- aind	mostrar indicador de atividade

Alvos:

- files	rastrear arquivos (padrão)
- no-files	não rastrear arquivos
- boots	rastrear setores de inicialização (padrão)
- no-boots	não rastrear setores de inicialização
- arch	rastrear arquivos compactados (padrão)
- no-arch	não rastrear arquivos compactados
- max-archive-level = LEVEL	NÍVEL máximo de encadeamento de arquivos
- scan-timeout = LIMIT	rastrear arquivos por LIMITE segundos no máximo. Se o tempo de rastreamento atingir esse limite, o rastreamento do arquivo compactado será interrompido e o rastreamento continuará no próximo arquivo.
- max-arch-size=SIZE	somente rastreia os primeiros bytes de TAMANHO em arquivos compactados (padrão 0 = sem limite)
- mail	rastrear arquivos de email
- no-mail	não rastrear arquivos de email
- sfx	rastrear arquivos compactados de autoextração
- no-sfx	não rastrear arquivos compactados de autoextração
- rtp	rastrear compactadores em tempo real
- no-rtp	não rastrear compactadores em tempo real
- exclude = FOLDER	excluir PASTA do rastreamento
- subdir	rastrear subpastas (padrão)
- no-subdir	não rastrear subpastas
- max-subdir-level = LEVEL	NÍVEL máximo de compactação de subpastas (padrão 0 = sem limite)
- symlink	seguir links simbólicos (padrão)
- no-symlink	ignorar links simbólicos
- ext-remove = EXTENSIONS	
- ext-exclude = EXTENSIONS	excluir do rastreamento EXTENSÕES delimitadas por dois-pontos

Métodos:

- adware	rastrear se há Adware/Spyware/Riskware
- no-adware	não rastrear se há Adware/Spyware/Riskware
- unsafe	rastrear por aplicativos potencialmente inseguros
- no-unsafe	não rastrear por aplicativos potencialmente não seguros
- unwanted	rastrear por aplicativos potencialmente indesejados
- no-unwanted	não rastrear por aplicativos potencialmente indesejados
- pattern	usar assinaturas
- no-pattern	não usar assinaturas
- heur	ativar heurística
- no-heur	desativar heurística
- adv-heur	ativar heurística avançada
- no-adv-heur	desativar heurística avançada

Limpeza:

- action = ACTION	executar AÇÃO em objetos infectados. Ações disponíveis: nenhum, limpar, aviso
- quarantine	copiar os arquivos infectados para Quarentena (completa AÇÃO)
- no-quarantine	não copiar arquivos infectados para Quarentena

Relatórios:

- log-file=FILE	registrar o relatório em ARQUIVO
- log-rewrite	substituir arquivo de saída (padrão – acrescentar)
- log-all	também registrar arquivos limpos
- no-log-all	não registrar arquivos limpos (padrão)

Possíveis códigos de saída do rastreamento:

0	- nenhuma ameaça encontrada
1	- ameaça encontrada mas não limpa
10	- alguns arquivos permanecem infectados
101	- erro no arquivo compactado
102	- erro de acesso
103	- erro interno

OBSERVAÇÃO: Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

4.2.1.5 Desempenho

Nesta seção, é possível definir o número de mecanismos de rastreamento do ThreatSense que serão usados para o rastreamento de vírus. Mais mecanismos de rastreamento do ThreatSense em máquinas com vários processadores podem aumentar a velocidade do rastreamento. O valor aceitável é 1-20.

Se não houver outras restrições, recomendamos aumentar o número de mecanismos de rastreamento ThreatSense na janela Configurações avançadas (F5) em **Proteção do computador** > **Antivírus e antispyware** > **Desempenho**, de acordo com esta fórmula: *número de mecanismos de rastreamento ThreatSense = (número de CPUs físicas x 2) + 1*. Veja um exemplo:

Suponhamos que você tenha um servidor com 4 CPUs físicas. Para o melhor desempenho, de acordo com a fórmula anterior, você deve ter 9 mecanismos de rastreamento.

OBSERVAÇÃO: As alterações feitas aqui serão aplicadas somente após a reinicialização.

4.2.1.6 Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos POP3 e HTTP é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. O controle funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. As seguintes opções estão disponíveis para a filtragem de protocolos (se a opção **Ativar filtragem de conteúdo do protocolo de aplicativo** estiver selecionada):

Portas HTTP e POP3s – Limita o rastreamento da comunicação às portas HTTP e POP3 conhecidas.

Aplicativos marcados como navegadores da Internet e clientes de email – Ative essa opção para filtrar somente a comunicação de aplicativos marcados como navegadores (**Proteção do acesso à Web** > **HTTP, HTTPS** > **Navegadores Web**) e clientes de email (**Proteção do cliente de email** > **POP3, POP3s** > **Clientes de email**).

Portas e aplicativos marcados como navegadores da Internet ou clientes de email – Portas e navegadores são verificados quanto a malware.

OBSERVAÇÃO: Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 2008, um novo método de filtragem de comunicações está sendo usado. Como resultado, a seção Filtragem de protocolos não está disponível.

4.2.1.6.1 SSL

O ESET File Security permite verificar protocolos encapsulados no protocolo SSL. É possível usar vários modos de rastreamento para as comunicações protegidas por SSL utilizando certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Sempre rastrear o protocolo SSL – Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado sobre o fato e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado por você como confiável (ele será adicionado à lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

Perguntar sobre sites não visitados (exclusões podem ser definidas) – Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.

Não rastrear o protocolo SSL – Se essa opção estiver selecionada, o programa não rastreará as comunicações em SSL.

Caso o certificado não possa ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (**Filtragem de protocolos** > **SSL** > **Certificados**):

Perguntar sobre validade do certificado – Solicita que o usuário selecione uma ação a ser tomada.

Bloquear a comunicação que utiliza o certificado – Encerra a conexão com o site que utiliza o certificado.

Se o certificado for inválido ou estiver corrompido (**Filtragem de protocolos** > **SSL** > **Certificados**):

Perguntar sobre validade do certificado – Solicita que o usuário selecione uma ação a ser tomada.

Bloquear a comunicação que utiliza o certificado – Encerra a conexão com o site que utiliza o certificado.

4.2.1.6.1.1 Certificados confiáveis

Além do armazenamento integrado de Autoridades de certificação raiz confiáveis, onde o ESET File Security armazena os certificados confiáveis, é possível criar uma lista personalizada de certificados confiáveis que pode ser exibida em **Configuração avançada** (F5) > **Filtragem de protocolos** > **SSL** > **Certificados** > **Certificados confiáveis** .

4.2.1.6.1.2 Certificados excluídos

A seção Certificados excluídos contém certificados que são considerados seguros. O conteúdo das comunicações criptografadas usando os certificados da lista não será verificado quanto a ameaças. Recomendamos que exclua apenas os certificados da Web que são realmente seguros, e tenha certeza de que as comunicações que utilizam esses certificados não precisam ser verificadas.

4.2.1.7 Configuração de parâmetros do mecanismo ThreatSense

O ThreatSense é o nome da tecnologia que consiste em métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

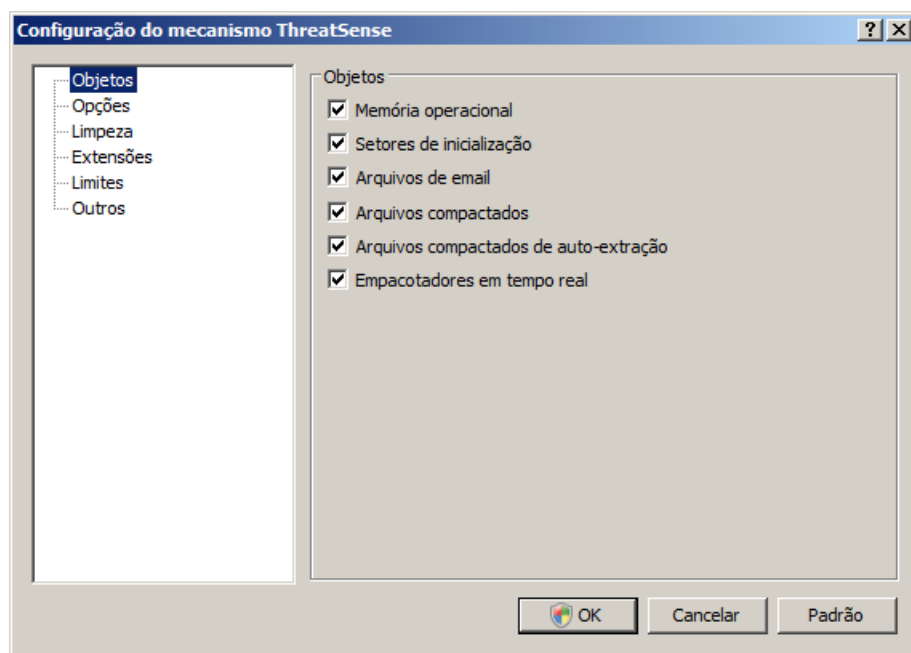
- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique no botão **Configuração...** localizado na janela de configuração de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos
- Rastrear arquivos na inicialização do sistema
- Proteção de email
- Proteção do acesso à web
- Rastreamento sob demanda do computador

Os parâmetros do ThreatSense são altamente otimizados para cada módulo e a modificação pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar heurística avançada no módulo da proteção em tempo real do sistema de arquivos pode resultar em lentidão do sistema (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastreamento sob demanda do computador.

4.2.1.7.1 Configuração de objetos

A seção **Objetos** permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

Memória operacional – Rastreia procurando ameaças que atacam a memória operacional do sistema.

Setores de inicialização – Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.

Arquivos – Fornece o rastreamento de todos os tipos de arquivos comuns (programas, imagens, áudio, arquivos de vídeo, arquivos de banco de dados etc.)

Arquivos de email – Rastreia arquivos especiais que contenham mensagens de email.

Arquivos compactados – Fornece o rastreamento de arquivos compactados (.rar, .zip, .arj, .tar, etc.).

Arquivos compactados de autoextração – Rastreia os arquivos contidos em arquivos compactados de autoextração, mas geralmente apresentados com a extensão de arquivo .exe

Empacotadores em tempo real – Diferente dos tipos de arquivos compactados padrão, os empacotadores em tempo real são descompactados na memória, além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FGS etc.).

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.2.1.7.2 Opções

Na seção **Opções**, é possível selecionar os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

Assinaturas – As assinaturas podem detectar e identificar infiltrações, com exatidão e segurança, por seus nomes usando as assinaturas de vírus.

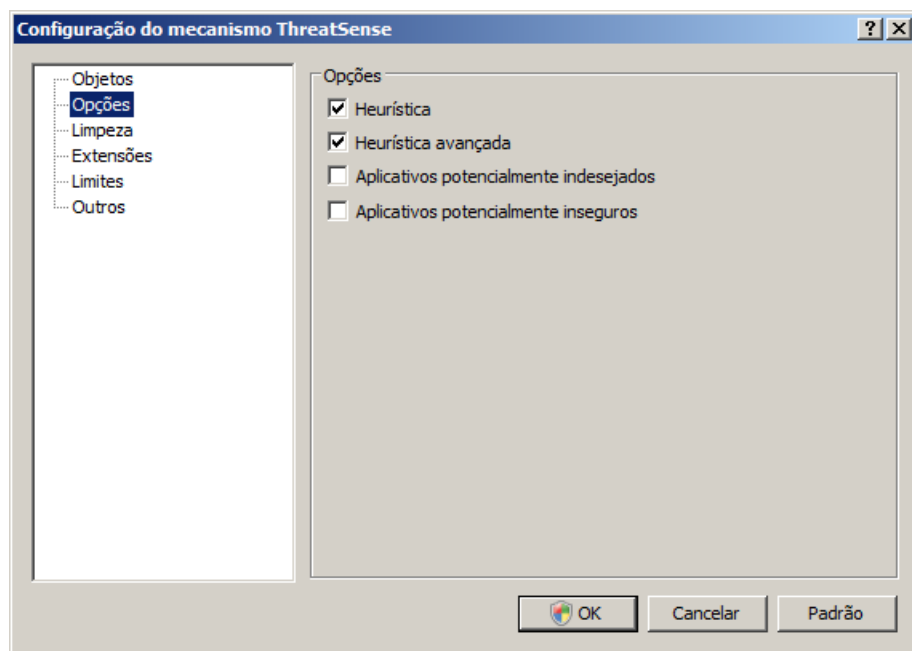
Heurística – A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (banco de dados de assinatura de vírus).

Heurística avançada – A heurística avançada é formada por um algoritmo heurístico exclusivo, desenvolvido pela ESET e otimizado para a detecção de worms e cavalos de troia de computador escritos em linguagens de programação de alto nível. Devido à heurística avançada, a inteligência da detecção do programa é

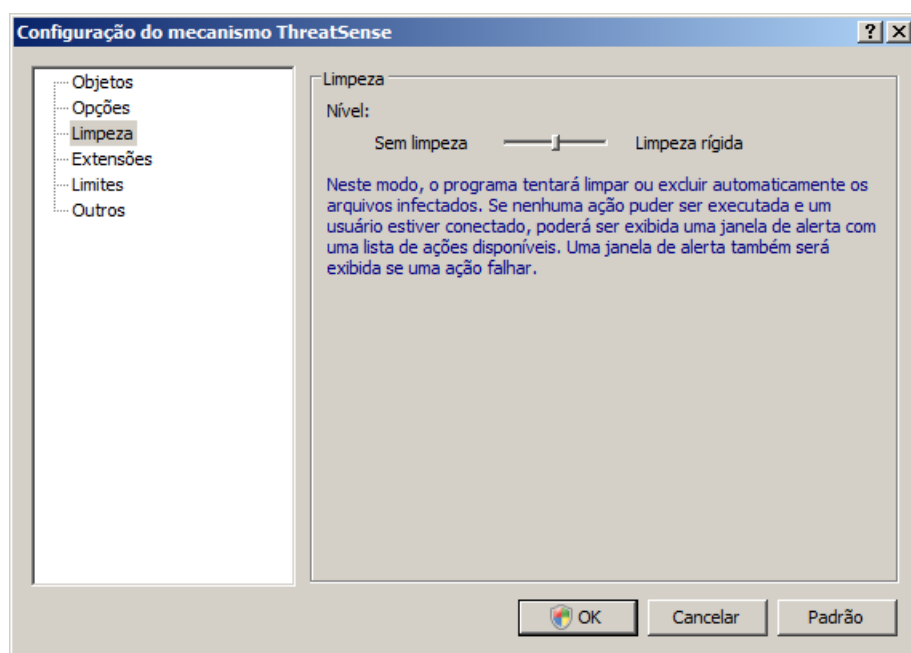
significativamente superior.

Adware/Spyware/Riskware – Essa categoria inclui o software que coleta várias informações confidenciais sobre usuários sem o consentimento informado deles. E inclui também software que exibe material de propaganda.

Aplicativos potencialmente indesejados – Aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem prejudicar o desempenho do computador. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.

Aplicativos potencialmente inseguros – Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Ela inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.2.1.7.3 Limpeza

As configurações de limpeza determinam o comportamento do scanner durante a limpeza dos arquivos infectados. Há três níveis de limpeza:

Sem limpeza – Os arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que você escolha uma ação.

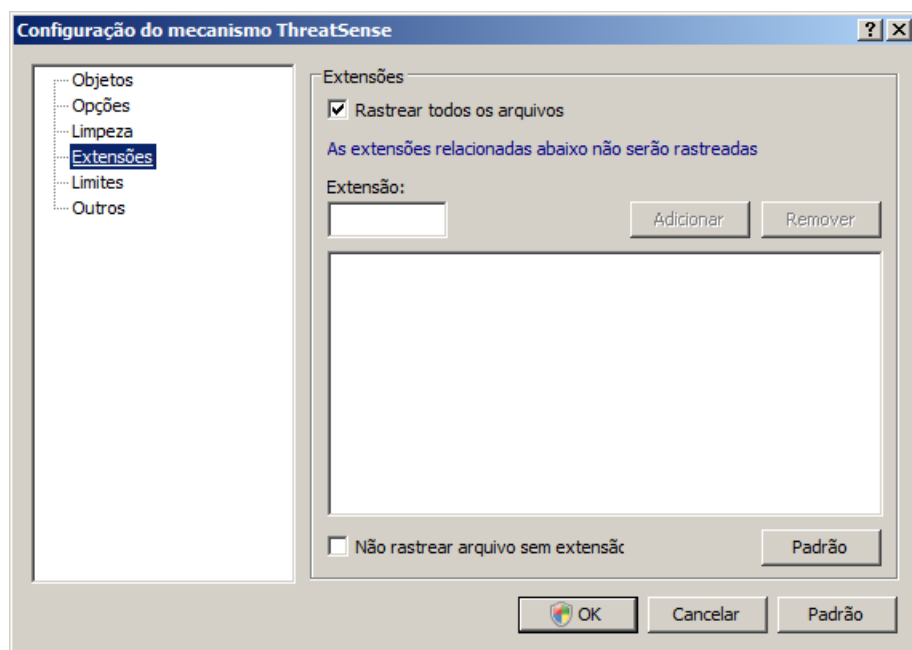
Limpeza padrão – O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma escolha de ações a serem seguidas. A escolha das ações a serem seguidas também será exibida se uma ação predefinida não for concluída.

Limpeza rígida – O programa limpará ou excluirá todos os arquivos infectados (incluindo os arquivos compactados). As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, será oferecida a você uma ação a ser tomada na janela de aviso.

Alerta: No modo Padrão, o arquivo compactado inteiro será excluído somente se todos os arquivos do arquivo compactado estiverem infectados. Se no arquivo compactado houver arquivos legítimos, ele não será excluído. Se um arquivo do arquivo compactado infectado for detectado no modo de Limpeza rígida, todo o arquivo compactado será excluído, mesmo se houver arquivos limpos.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.2.1.7.4 Extensões

Uma extensão é a parte do nome do arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Se a opção **Rastrear todos os arquivos** estiver desmarcada, a lista será alterada para exibir todas as extensões de arquivos rastreados no momento. Com os botões **Adicionar** e **Remover**, você pode habilitar ou desabilitar o rastreamento das extensões desejadas.

Para habilitar o rastreamento de arquivos sem nenhuma extensão, marque a opção **Rastrear arquivos sem extensão**.

A exclusão de arquivos do rastreamento será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando as extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.2.1.7.5 Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Tamanho máximo do objeto: – Define o tamanho máximo dos objetos que serão rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Não recomendamos alterar o valor padrão, pois não há razão para modificá-lo. Essa opção deverá ser alterada apenas por usuários avançados que tenham razões específicas para excluir objetos maiores do rastreamento.

Tempo máximo do rastreamento para objeto (s): – Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento.

Nível de compactação de arquivos: – Especifica a profundidade máxima do rastreamento de arquivos compactados. Não recomendamos alterar o valor padrão de 10; sob circunstâncias normais, não haverá razão para modificá-lo. Se o rastreamento for encerrado prematuramente devido ao número de arquivos compactados aninhados, o arquivo compactado permanecerá desmarcado.

Tamanho máximo do arquivo no arquivo compactado: – Essa opção permite especificar o tamanho máximo dos

arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Se o rastreamento de um arquivo compactado for encerrado prematuramente por essa razão, o arquivo compactado permanecerá sem verificação.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.2.1.7.6 Outros

Rastrear fluxos dados alternativos (ADS) – Os fluxos de dados alternativos (ADS) usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar rastreamento em segundo plano com baixa prioridade – Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.

Registrar todos os objetos – Se essa opção estiver selecionada, o arquivo de relatório mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados.

Ativar otimização inteligente –Selecione essa opção para que os arquivos que já foram rastreados não sejam rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus.

Manter último registro de acesso – Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (ou seja, para uso com sistemas de backup de dados).

Relatório de rolagem – Essa opção permite ativar/desativar o rolamento do relatório. Se selecionada, as informações rolam para cima dentro da janela de exibição.

Exibir notificação sobre a conclusão do rastreamento em uma janela separada – Abre uma janela autônoma que contém as informações sobre os resultados do rastreamento.

OBSERVAÇÃO: Quando um ponto azul for mostrado ao lado de um parâmetro, isso significa que o ajuste atual para esse parâmetro diferente do ajuste de outros módulos que também usam o ThreatSense. Como você pode configurar o mesmo parâmetro de forma diferente para cada módulo, esse ponto azul apenas o lembra de que esse mesmo parâmetro é configurado de forma diferente para outros módulos. Se não houver um ponto azul, o parâmetro para todos os módulos é configurado da mesma forma.

4.2.1.8 Uma infiltração foi detectada

As infiltrações podem alcançar o sistema a partir de vários pontos: páginas da Web, arquivos compartilhados, email ou dispositivos de computador removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET File Security e clique em Rastreamento do computador
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte a seção Rastreamento inteligente)
- Após o rastreamento ter terminado, revise o relatório para informações como número dos arquivos verificados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Como exemplo geral de como as infiltrações são tratadas no ESET File Security, suponha que uma infiltração seja detectada pelo monitor do sistema de arquivos em tempo real, que usa o nível de limpeza Padrão. Ele tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida a ser tomada para o módulo de proteção em tempo real, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Deixar** estão disponíveis. A seleção da opção **Deixar** não é recomendada, visto que os arquivos infectados seriam mantidos intactos. A exceção a isso é quando você tem certeza de que o arquivo é inofensivo e foi detectado por engano.

Limpeza e exclusão – Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou, a esse arquivo, um código malicioso. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso pelo processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

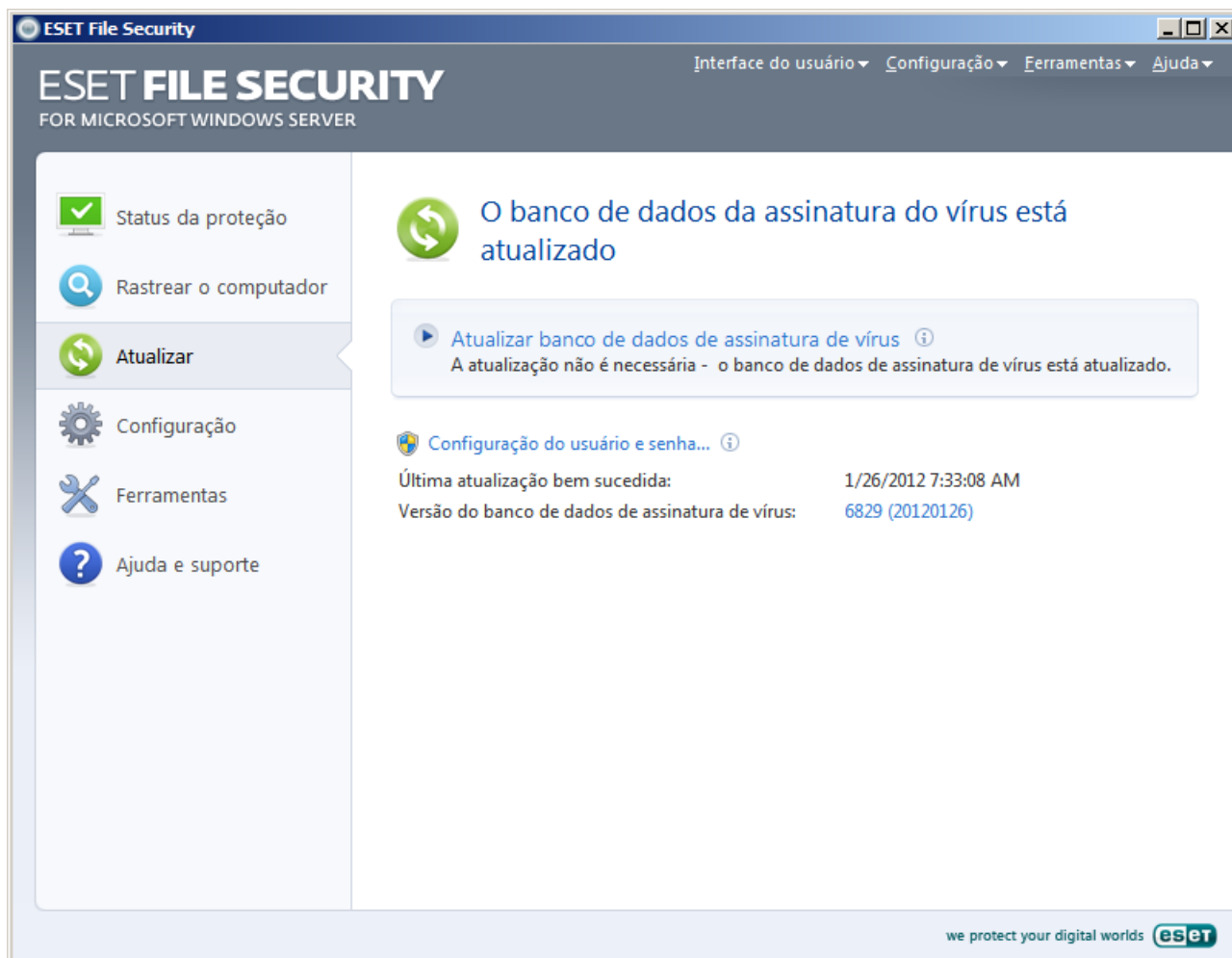
Exclusão de arquivos em arquivos compactados – No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Entretanto, use precaução ao executar um rastreamento com Limpeza rígida – com esse tipo de limpeza, o arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

4.3 Atualização do programa

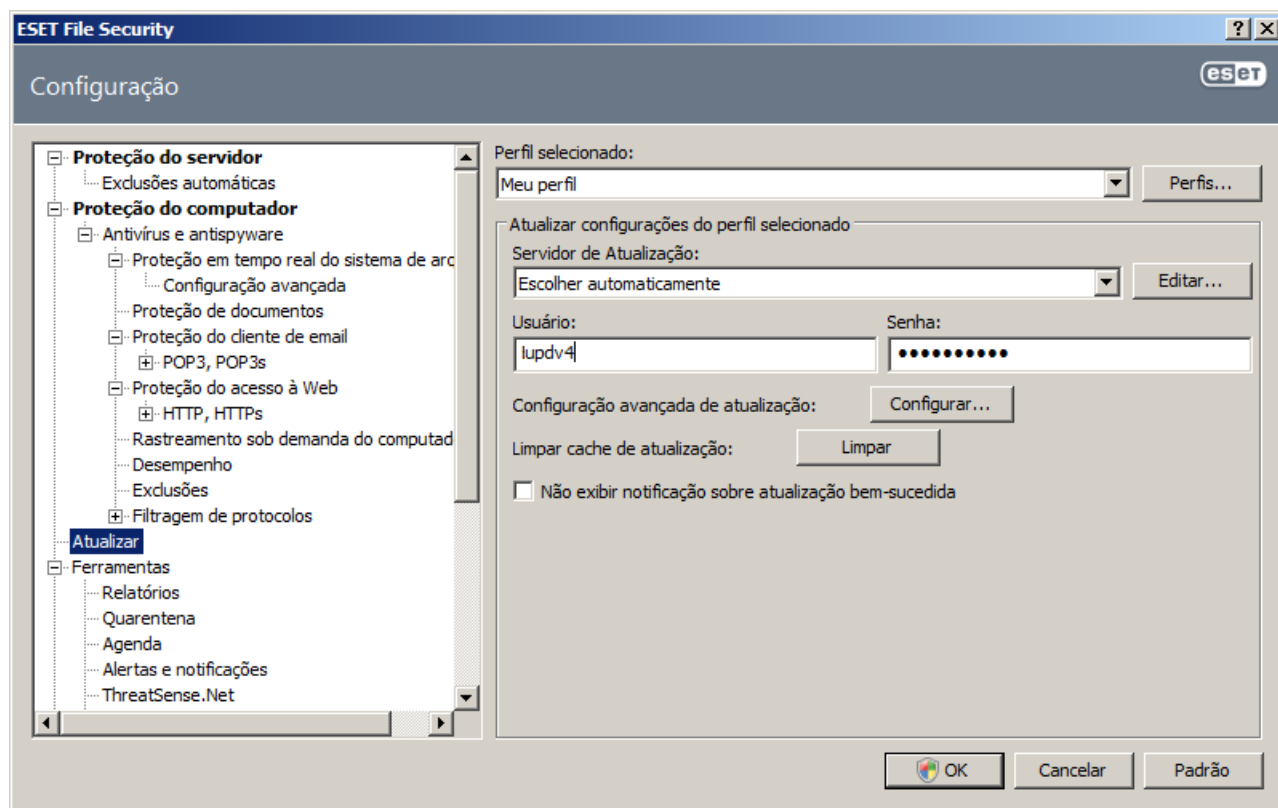
A atualização regular do ESET File Security é a premissa básica para obter o nível máximo de segurança. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras: atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

No menu principal, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

Além disso, a opção para iniciar o processo de atualização manualmente - **Atualizar banco de dados de assinatura de vírus** - está disponível, bem como as opções de configuração básica das atualizações, como o nome de usuário e a senha, para acessar os servidores de atualização da ESET.

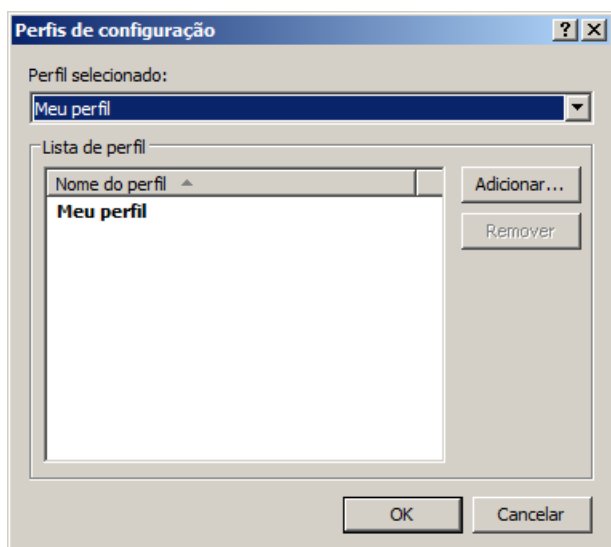
Use o link **Ativação do produto** para abrir o formulário de registro que ativará o seu produto de segurança da ESET e enviará a você um email com seus dados de autenticação (nome de usuário e senha).

OBSERVAÇÃO: O nome de usuário e a senha são fornecidos pela ESET após a compra do ESET File Security.

4.3.1 Configuração da atualização

A seção de configuração da atualização especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o menu suspenso **Servidor de atualização** está configurado para **Escolher automaticamente**, a fim de garantir que os arquivos de atualização sejam obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede. As opções de configuração da atualização estão disponíveis na árvore Configuração avançada (tecla F5), em **Atualizar**.

A lista de servidores de atualização disponíveis pode ser acessada pelo menu suspenso **Servidor de atualização**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**. A autenticação dos servidores de atualização é baseada no **Usuário** e na **Senha** gerados e enviados a você após a compra.

4.3.1.1 Atualizar perfis

É possível criar perfis de atualização para várias configurações e tarefas de atualização. A criação de perfis de atualização é particularmente útil para usuários móveis, que podem criar um perfil alternativo para propriedades de conexão à Internet que são alteradas com frequência.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento, definido como o **Meu perfil** por padrão. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e insira seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar as configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil**.

Na janela de configuração de perfil, especifique o servidor de atualização a partir de uma lista de servidores disponíveis ou adicione um novo servidor. A lista de servidores de atualização existentes pode ser acessada no menu suspenso **Servidor de atualização**: Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**.

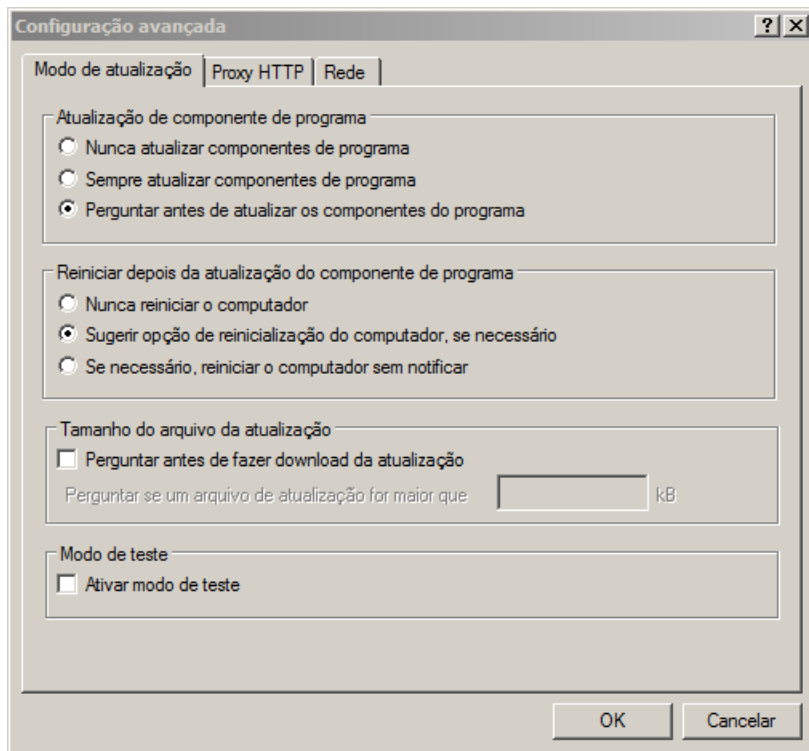
4.3.1.2 Configuração avançada de atualização

Para exibir a Configuração avançada de atualização, clique no botão **Configuração...**. As opções de configuração avançada de atualização incluem a configuração do **Modo de atualização**, **Proxy HTTP**, **Rede** e **Imagem**.

4.3.1.2.1 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa.

Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Nunca atualizar componentes de programa**: As novas atualizações de componentes do programa não serão obtidas por download.
- **Sempre atualizar componentes de programa**: As novas atualizações de componentes do programa serão feitas automaticamente.
- **Perguntar antes de fazer download dos componentes de programa**: A opção padrão. Você será solicitado a confirmar ou recusar as atualizações de componentes do programa quando elas estiverem disponíveis.

Após a atualização de componentes do programa, poderá ser necessário reiniciar o computador para obter uma completa funcionalidade de todos os módulos. A seção **Reiniciar depois da atualização do componente de programa** permite que o usuário selecione uma das seguintes opções:

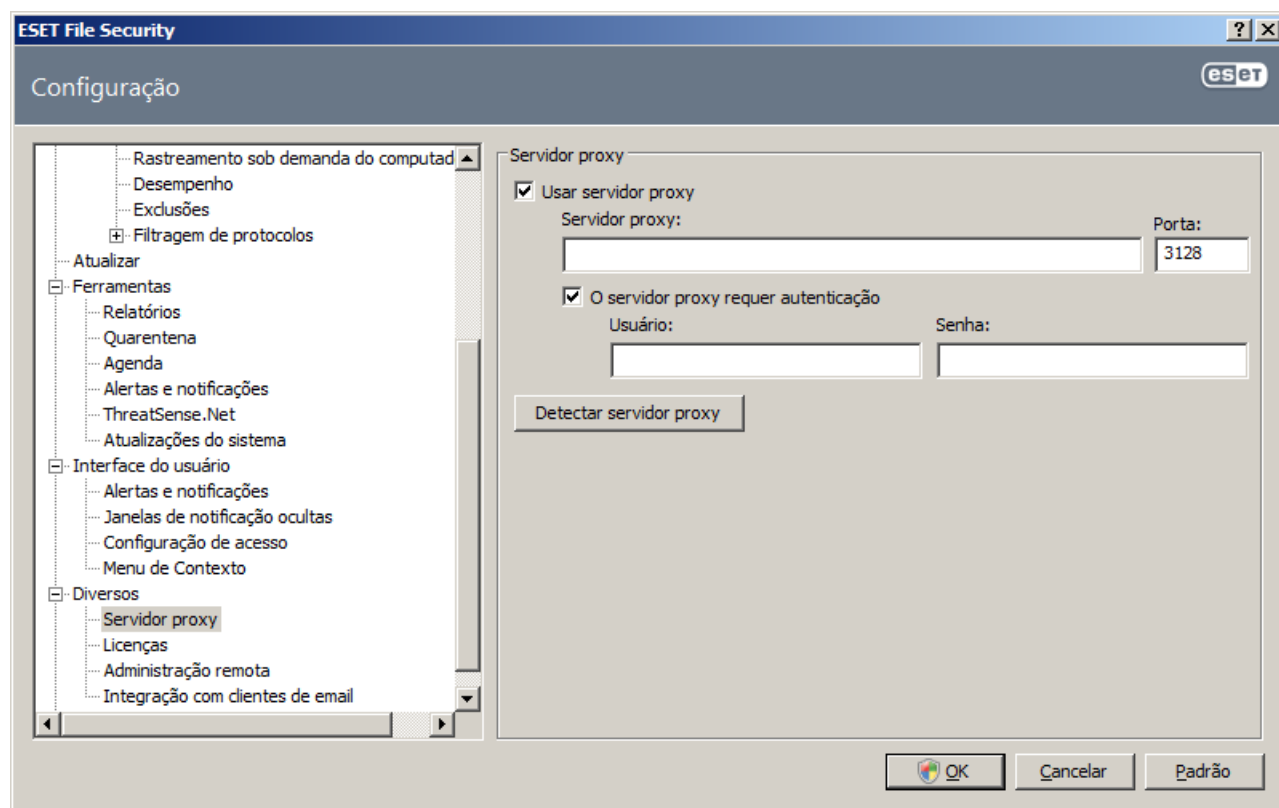
- **Nunca reiniciar o computador**
- **Sugerir opção de reinicialização do computador, se necessário**
- **Se necessário**, **reinicialize o computador sem notificação**

A opção padrão é **Sugerir opção de reinicialização do computador, se necessário**. A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

4.3.1.2.2 Servidor proxy

No ESET File Security, a configuração do servidor proxy está disponível em duas seções diferentes na árvore Configuração avançada.

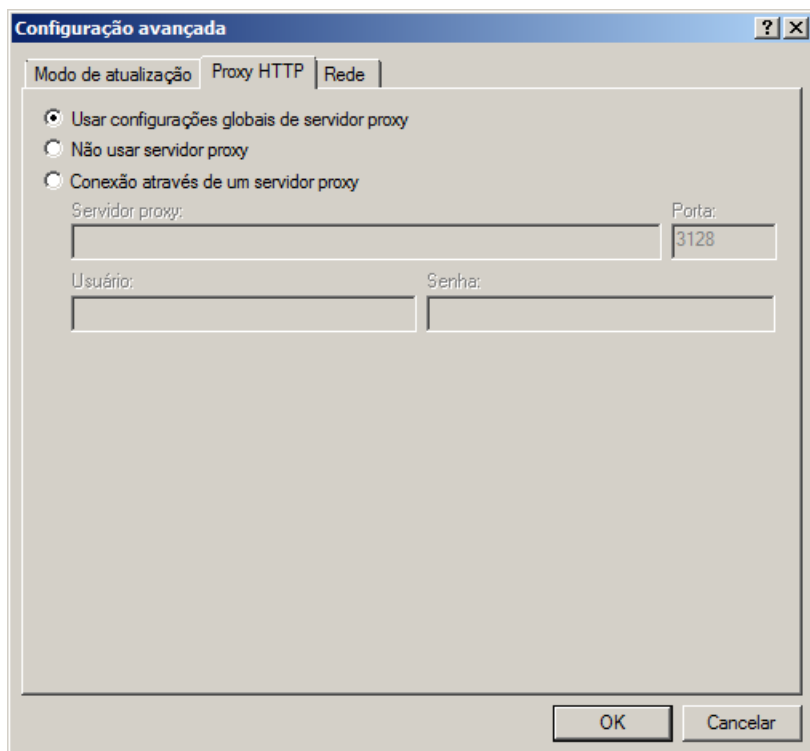
Primeiramente, as configurações do servidor proxy podem ser definidas em **Diversos** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET File Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**: além do número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy requerer autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos. Clique no botão **Detectar servidor proxy** para detectar e inserir automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

OBSERVAÇÃO: Esse recurso não recupera dados de autenticação (nome de usuário e senha), que devem ser fornecidos por você.

As configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização. Essa configuração será aplicada ao perfil de atualização determinado. É possível acessar as opções de configuração do servidor proxy de determinado perfil de atualização clicando na guia **Proxy HTTP** na **Configuração avançada de atualização**. Você terá uma destas três opções:

- **Usar configurações globais de servidor proxy**
- **Não usar servidor proxy**
- **Conexão através de um servidor proxy** (conexão definida pelas propriedades de conexão)

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Diversos** > **Servidor proxy** da árvore Configuração avançada (descritas no início desse artigo).

Selecione a opção **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET File Security.

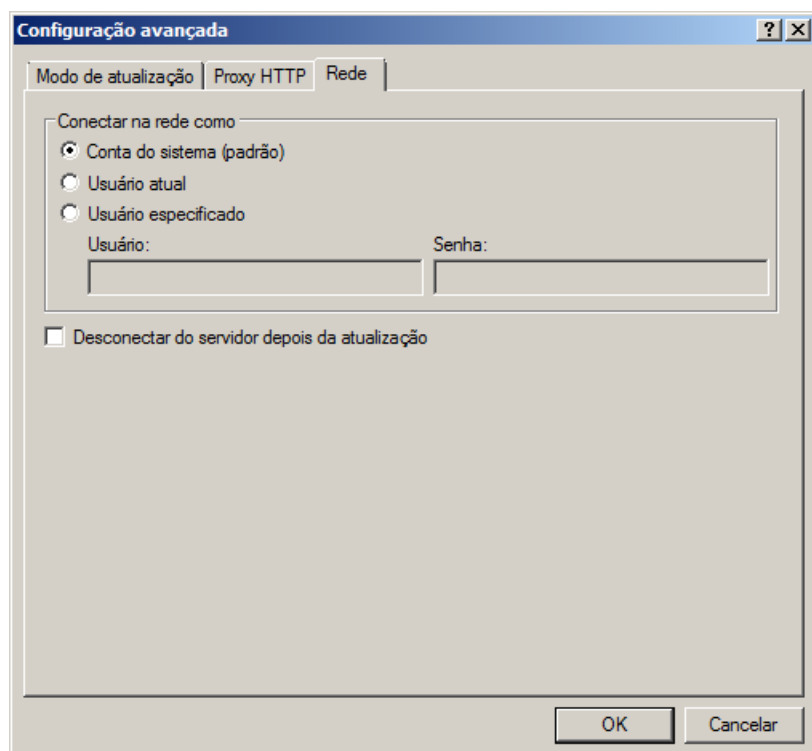
A opção **Conexão através de um servidor proxy** deve ser selecionada se um servidor proxy for usado para atualizar o ESET File Security e for diferente do servidor proxy especificado nas configurações globais (**Diversos** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação, além do **Usuário** e da **Senha** para o servidor proxy, se necessário.

Essa opção também deve ser selecionada se as configurações do servidor proxy não tiverem sido definidas globalmente, mas o ESET File Security se conectará a um servidor proxy para obter atualizações.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

4.3.1.2.3 Conexão à rede

Ao atualizar a partir de um servidor local com um sistema operacional baseado em NT, a autenticação para cada conexão de rede é necessária por padrão. Na maioria dos casos, a conta do sistema local não tem direitos de acesso suficientes para a pasta Imagem, que contém cópias dos arquivos de atualização. Se esse for o caso, insira o nome de usuário e a senha na seção de configuração da atualização ou especifique uma conta na qual o programa acessará o servidor de atualização (Imagem).

Para configurar essa conta, clique na guia **Rede**. A seção **Conectar à rede como** oferece as opções **Conta do sistema** (**padrão**), **Usuário atual** e **Usuário especificado**.

Selecione a opção **Conta do sistema** (**padrão**) para usar a conta do sistema para autenticação. Normalmente, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

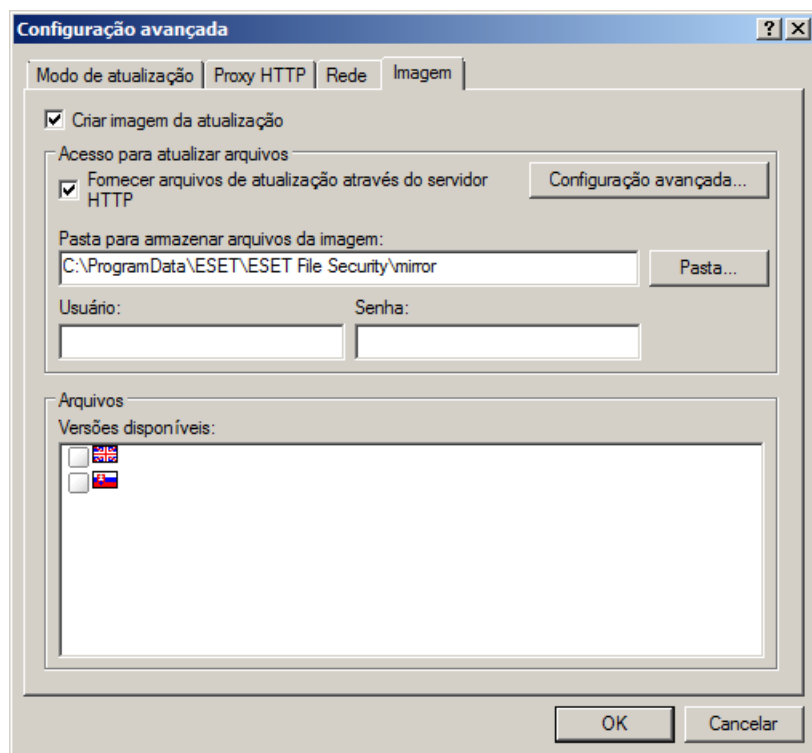
Para assegurar que o programa seja autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação.

Alerta: Quando a opção **Usuário atual** ou **Usuário especificado** estiver ativada, um erro pode ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: nome_domínio\usuário (se for um grupo de trabalho, insira nome do_grupo de trabalho_nome\nome) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

4.3.1.2.4 Criação de cópias de atualização - Imagem

O ESET File Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outras estações de trabalho localizadas na rede. A atualização das estações clientes a partir de uma Imagem otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração do servidor local da Imagem podem ser acessadas (após a inserção da chave de licença válida no gerenciador de licenças, localizado na seção Configuração avançada do ESET File Security) na seção **Configuração avançada de atualização**: Para acessar essa seção, pressione F5 e clique no botão **Atualizar** na árvore Configuração avançada, depois clique no botão **Configuração...** ao lado de **Configuração avançada de atualização**: e selecione a guia **Imagem**).

A primeira etapa na configuração da Imagem é selecionar a opção Criar imagem de atualização. A seleção dessa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Os métodos de ativação da Imagem estão descritos em detalhes na seção Atualização através da Imagem. Por enquanto, observe que há dois métodos básicos para acessar a Imagem - a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta...** para procurar uma pasta no computador local ou em uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome do usuário** e **Senha**. O nome do usuário e a senha devem ser inseridos no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Ao configurar a Imagem, também é possível especificar as versões de idioma dos quais se deseja fazer download das cópias de atualização. A configuração da versão de idioma pode ser acessada na seção **Arquivos** - **Versões disponíveis**:.

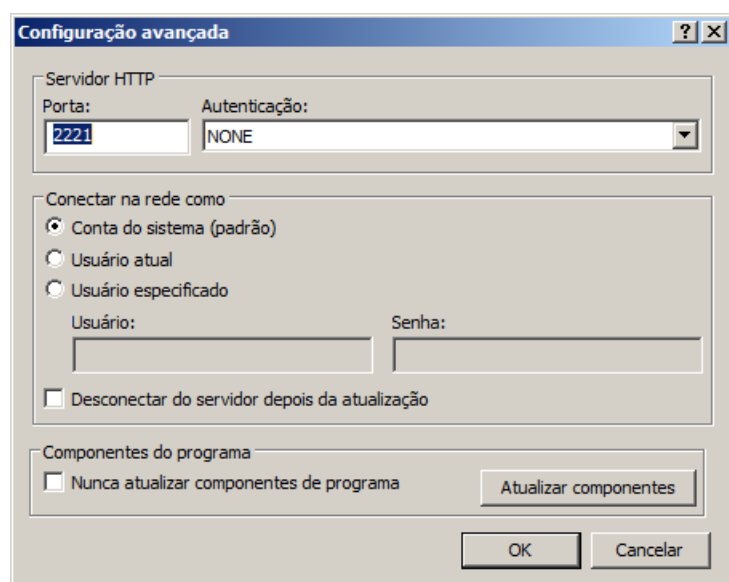
4.3.1.2.4.1 Atualização através da Imagem

Há dois métodos básicos para configurar a Imagem – a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

Acesso à Imagem utilizando um servidor HTTP interno

Essa é a configuração padrão especificada na configuração do programa predefinida. Para permitir o acesso à Imagem utilizando o servidor HTTP, navegue até **Configuração avançada de atualização** (guia **Imagem**) e selecione a opção **Criar imagem da atualização**.

Na seção **Configuração avançada** da guia **Imagem**, é possível especificar a **Porta do servidor** em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**. A opção **Autenticação** define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **NENHUM**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **NENHUM**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Alerta: Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Imagem deve estar localizada no mesmo computador que a instância do ESET File Security que os criou.

Após concluir a configuração da Imagem, vá até as estações de trabalho e adicione um novo servidor de atualização no formato **http://endereço_IP_do_seu_servidor:2221**. Para fazer isso, siga as etapas a seguir:

- Abra a **Configuração avançada** do ESET File Security e clique na ramificação **Atualizar**.
- Clique em **Editar...** à direita do menu suspenso **Atualizar servidor** e adicione um novo servidor utilizando o seguinte formato: http://endereço_IP_do_seu_servidor:2221.
- Selecione esse servidor recém-adicionado na lista de servidores de atualização.

Acesso à Imagem por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um local ou em um dispositivo de rede. Ao criar a pasta para a Imagem, é necessário fornecer acesso de "gravação" para o usuário que salvará os arquivos de atualização na pasta e acesso de "leitura" para todos os usuários que atualizarão o ESET File Security a partir da pasta Imagem.

Depois, configure o acesso à Imagem na seção **Configuração avançada de atualização** (guia **Imagem**) desativando a opção **Fornecer arquivos de atualização através do servidor HTTP** . Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, será necessário especificar os dados de autenticação para acessar o outro computador. Para especificar os dados de autenticação, abra a Configuração avançada (F5) do ESET File Security e clique na ramificação **Atualizar**. Clique no botão **Configuração...** e clique na guia **Rede**. Essa configuração é a mesma para a atualização, conforme descrito na seção Conexão à rede.

Após concluir a configuração da Imagem, prossiga até as estações de trabalho e configure \\UNC\PATH como o servidor de atualização. Essa operação pode ser concluída seguindo estas etapas:

- Abra a Configuração avançada do ESET File Security e clique em **Atualizar**.
- Clique em **Editar...** ao lado de Atualizar servidor e adicione um novo servidor utilizando *formato \\UNC\PATH*.
- Selecione esse servidor recém-adicionado na lista de servidores de atualização

OBSERVAÇÃO: Para o funcionamento correto, o caminho para a pasta Imagem deve ser especificado como um caminho UNC. A atualização das unidades mapeadas pode não funcionar.

4.3.1.2.4.2 Solução de problemas de atualização através da Imagem

Na maioria dos casos, os problemas que ocorrem durante a atualização do servidor de Imagem são causados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Imagem, dados de autenticação incorretos para a pasta Imagem, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização na Imagem ou por uma combinação dessas razões citadas. Aqui é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Imagem:

O ESET File Security **relata um erro ao conectar a um servidor de imagem** - Provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no menu **Iniciar** do Windows, clique em **Executar**, insira o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.

O ESET File Security **requer um nome de usuário e senha** - Provavelmente provocado provocado por dados de autenticação incorretos (nome de usuário e senha) na seção de atualização. O nome do usuário e a senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, *Domínio/Nome de usuário* ou *Grupo de trabalho/Nome de usuário*, além das senhas correspondentes. Se o servidor de Imagem puder ser acessado por "Todos", esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. "Todos" não significa qualquer usuário não autorizado, apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta puder ser acessada por "Todos", um nome de usuário e uma senha ainda precisarão ser inseridos na seção de configuração da atualização.

O ESET File Security **relata um erro ao conectar a um servidor de imagem** – A comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

4.3.2 Como criar tarefas de atualização

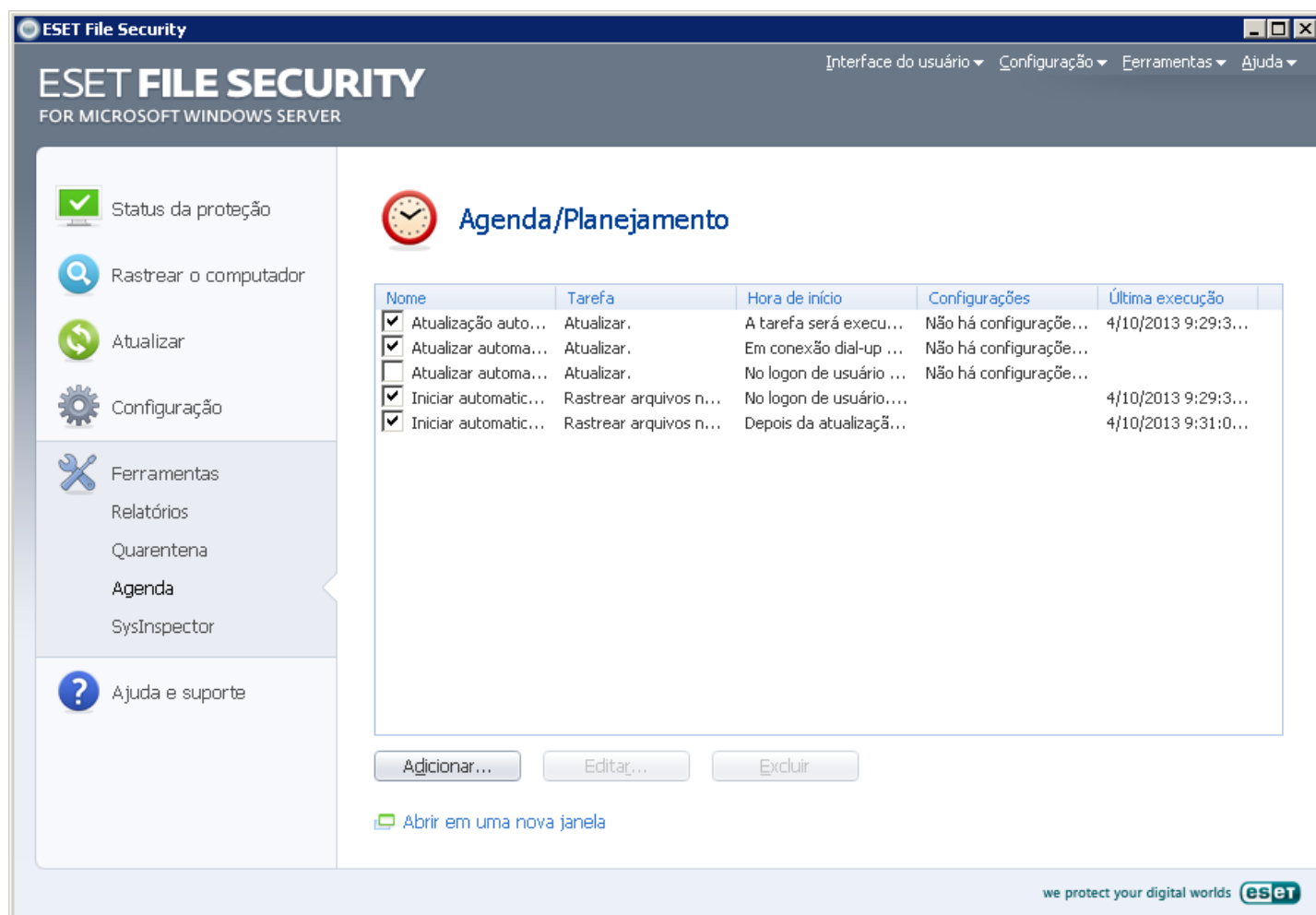
As atualizações podem ser disparadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em Atualizar no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas são ativadas no ESET File Security:

- **Atualização automática de rotina**
- **Atualizar automaticamente após conexão dial-up**
- **Atualizar automaticamente após logon do usuário**

Cada tarefa de atualização pode ser alterada de acordo com suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda.

4.4 Agenda

A Agenda ficará disponível se o Modo avançado no ESET File Security estiver ativado. A **Agenda** pode ser encontrada no menu principal do ESET File Security em **Ferramentas**. A Agenda contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Atualização automática de rotina**
- **Atualizar automaticamente após conexão dial-up**
- **Atualizar automaticamente após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema (após logon do usuário)**
- **Rastreamento de arquivos em execução durante inicialização do sistema (após atualização bem sucedida do banco de dados de assinatura de vírus)**

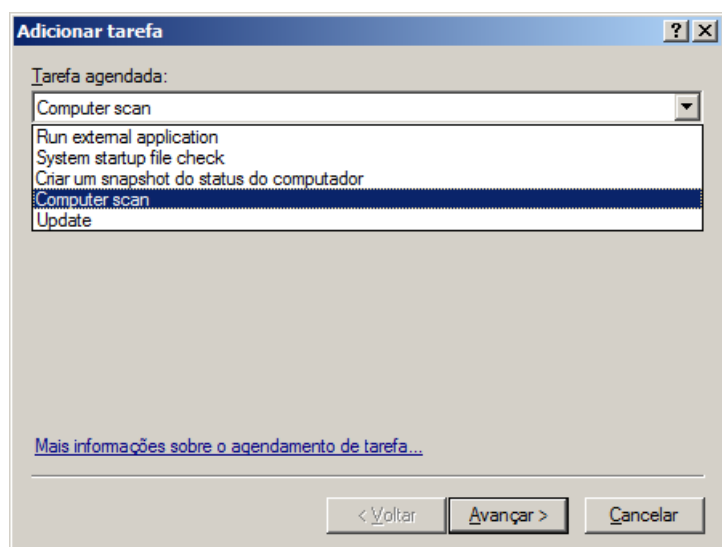
Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar...**.

4.4.1 Finalidade do agendamento de tarefas

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

4.4.2 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo**
- **Rastrear arquivos na inicialização do sistema**
- **Criar um snapshot do status do computador**
- **Rastreamento sob demanda do computador**
- **Atualizar**

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, nós explicaremos como adicionar uma nova tarefa de atualização.

No menu suspenso **Tarefa agendada**: selecione **Atualizar**. Clique em **Avançar** e insira o nome da tarefa no campo **Nome da tarefa**: Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Evento disparado**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você. Depois defina a ação a ser adotada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

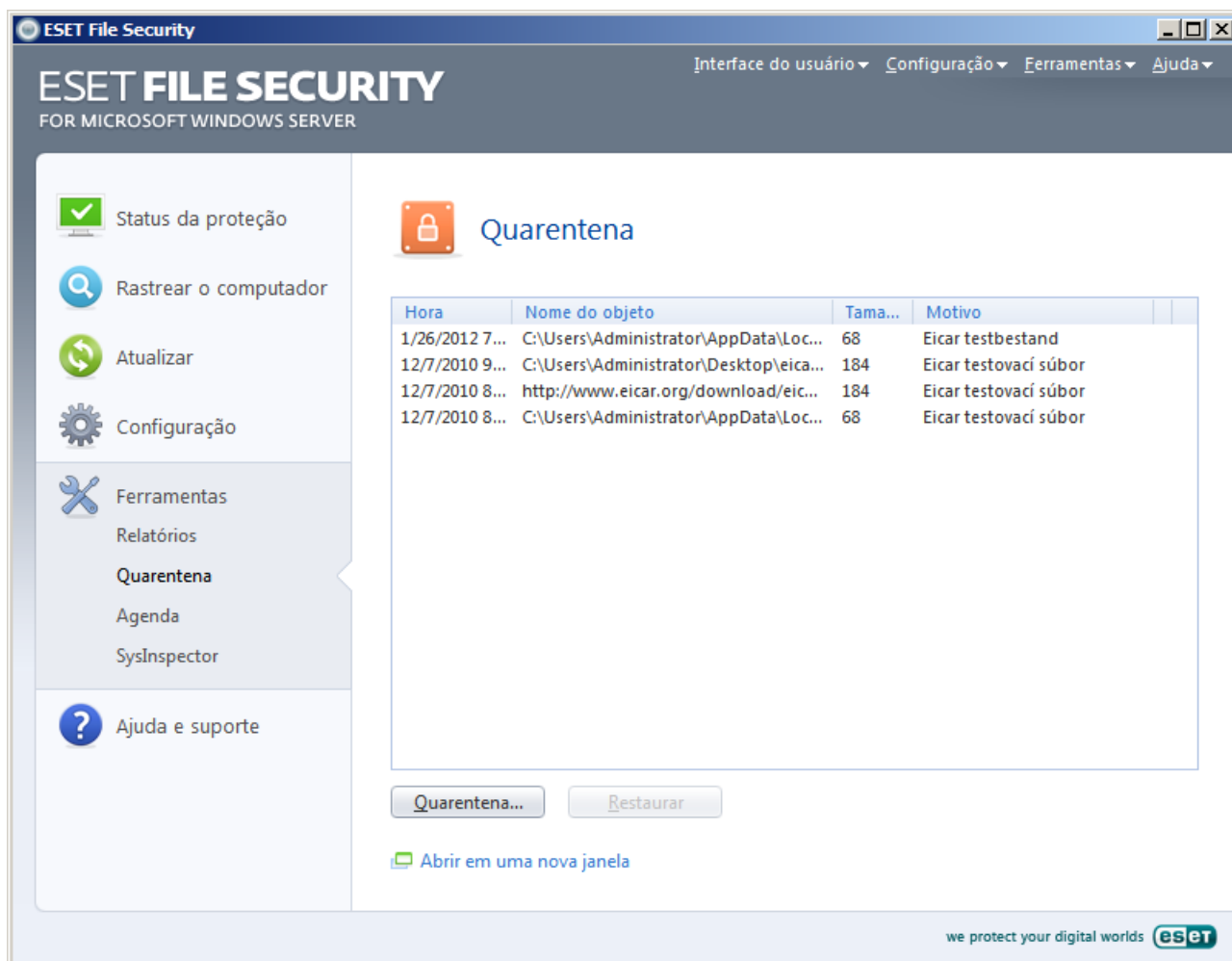
- **Aguardar até a próxima hora agendada**
- **Executar a tarefa tão logo quanto possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido utilizando a caixa de rolagem Intervalo da tarefa)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual será exibida; a opção **Executar a tarefa com parâmetros específicos** deve ser ativada automaticamente. Clique no botão **Concluir**.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo, que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **OK** na janela **Atualizar perfis**. A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

4.5 Quarentena

A principal tarefa da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET File Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo verificador antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de ameaças da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (**adicionado pelo usuário...**) e o número de ameaças (por exemplo, se ele for um arquivo compactado que contém diversas infiltrações).

4.5.1 Colocação de arquivos em quarentena

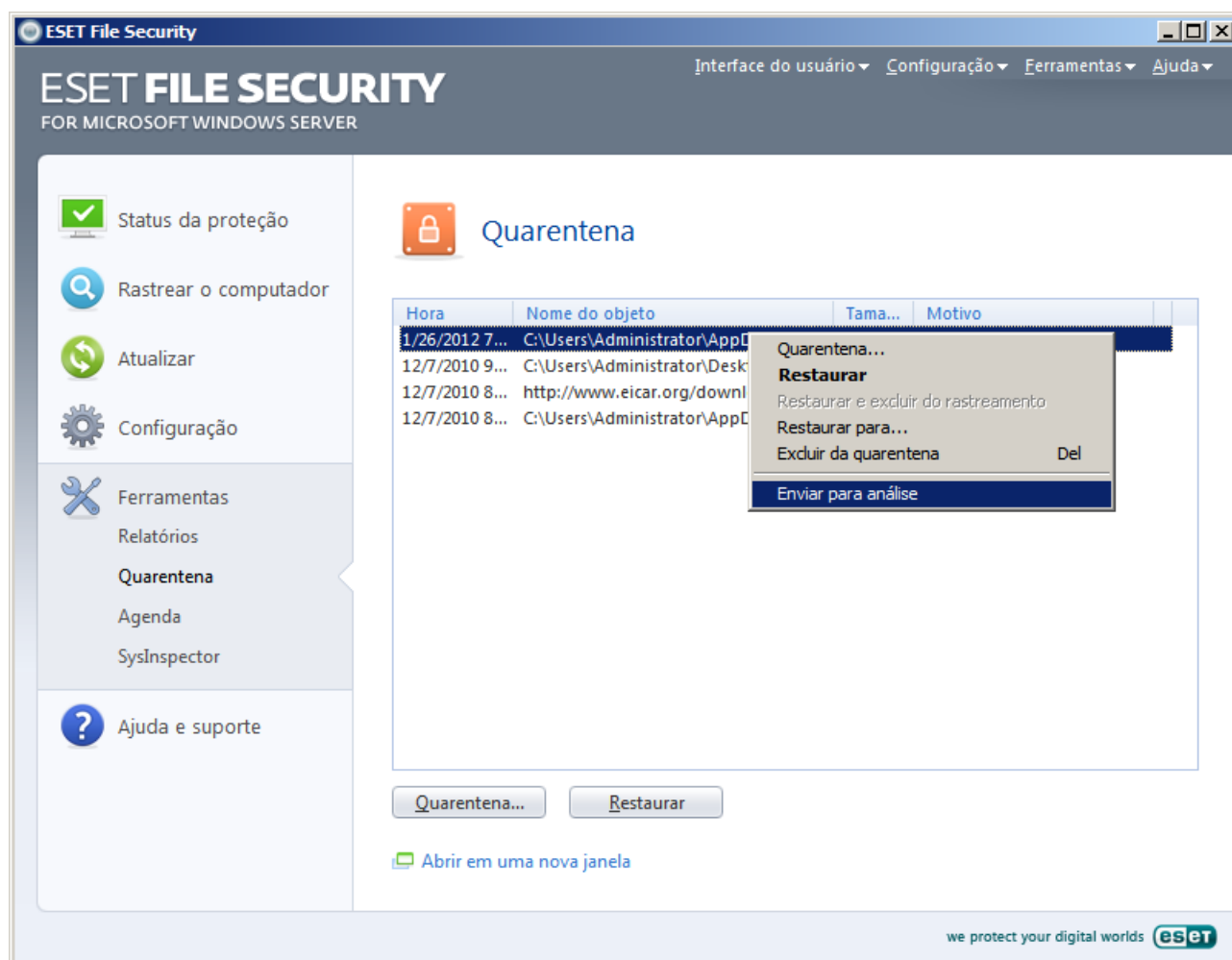
O ESET File Security coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando no botão **Quarentena...**. Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Adicionar...**

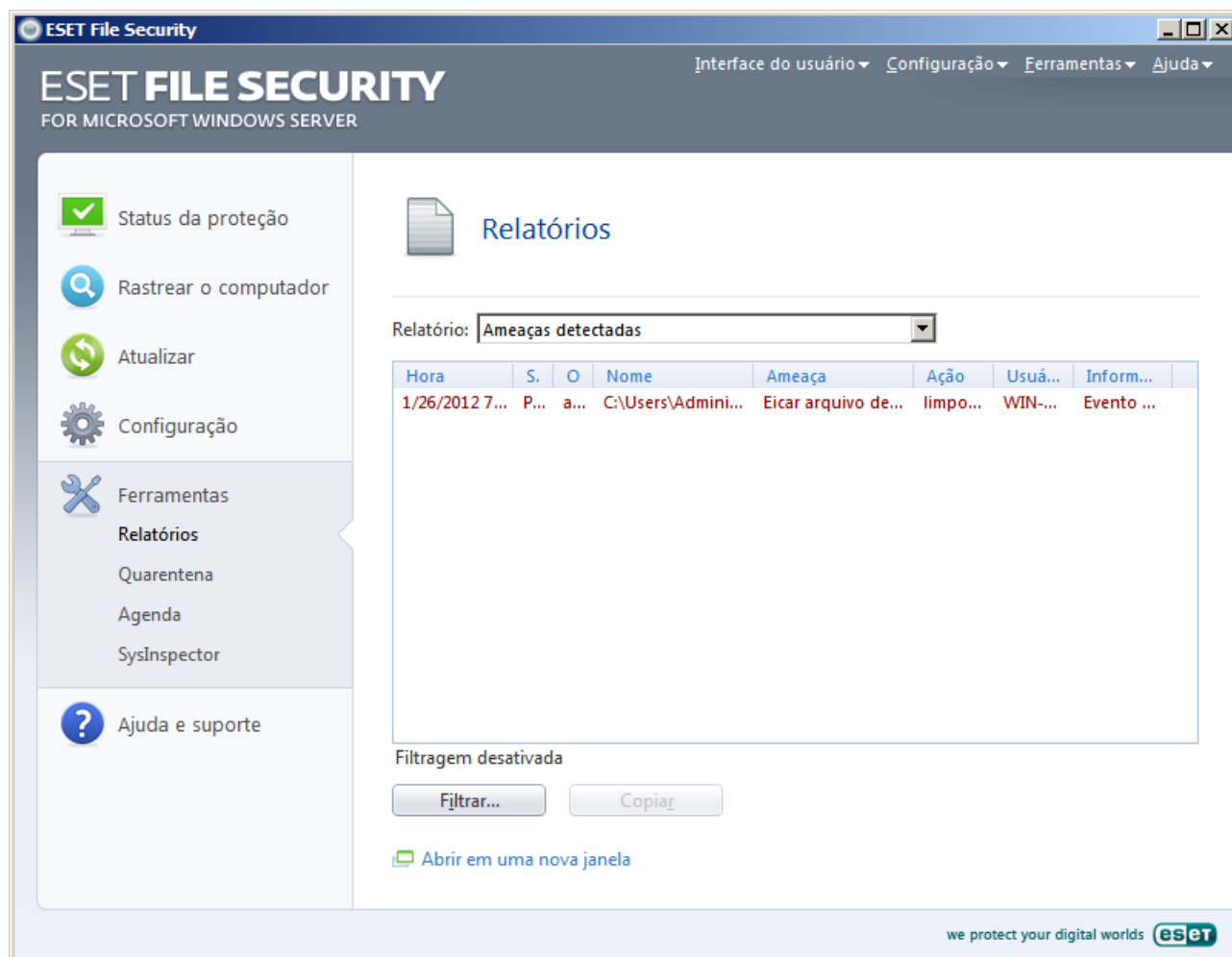
4.5.2 Restauração da Quarentena

Os arquivos colocados em quarentena podem ser restaurados para o local original. Para tanto, use o recurso **Restaurar**. A opção **Restaurar** está disponível no menu de contexto ao clicar com o botão direito do mouse no arquivo em questão na janela Quarentena. O menu de contexto oferece também a opção **Restaurar para**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO: Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

4.5.3 Envio de arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o Laboratório de ameaças da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

4.6 Relatórios

Os Relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas. Os Relatórios atuam como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. Os Relatórios são realizados ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do relatório. É possível visualizar mensagens de texto e relatórios diretamente do ambiente do ESET File Security.

Os relatórios podem ser acessados no menu principal, clicando em **Ferramentas** > **Relatórios**. Selecione o tipo de relatório desejado usando o menu suspenso **Relatório**: na parte superior da janela. Os seguintes relatórios estão disponíveis:

- **Ameaças detectadas** - Use esta opção para visualizar todas as informações sobre eventos relacionados a infiltrações detectadas, exceto infiltrações detectadas por rastreamento sob demanda do computador (esses eventos são registrados no relatório **Rastreamento sob demanda do computador**).
- **Eventos** - Essa opção foi desenvolvida para a solução de problemas de administradores do sistema e usuários. Todas as ações importantes executadas pelo ESET File Security são registradas nos Relatórios de eventos.
- **Rastreamento sob demanda do computador** - os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo Rastreamento sob demanda.

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão **Copiar**. Para selecionar várias entradas, use as teclas CTRL e SHIFT.

4.6.1 Filtragem de relatórios

A filtragem de relatórios é um recurso útil que o ajuda a encontrar registros nos relatórios, especialmente quando há muitos registros e é difícil encontrar a informação específica que você precisa.

Ao usar a filtragem, digite uma cadeia de caracteres **O que** para filtrar, especificar em quais **colunas procurar**, selecionar os **Tipos de registro** e definir um **Período de tempo** para limitar a quantidade de registros. Ao especificar determinadas opções de filtragem, apenas os registros relevantes (de acordo com as opções de filtragem) serão exibidos na janela **Relatórios** para acesso rápido e fácil.

Para abrir a janela **Filtragem de relatórios**, pressione o botão **Filtrar...** uma vez em **Ferramentas** > **Relatórios** ou use as teclas de atalho Ctrl + Shift + F.

OBSERVAÇÃO: Para pesquisar um registro específico, você pode usar o recurso Localizar no relatório ou em conjunto com a Filtragem de relatórios.

Ao especificar determinadas opções de filtro, apenas os registros relevantes (de acordo com as opções de filtragem) serão exibidos na janela Relatórios. Isso preencherá/limitará a quantidade de registros, fazendo, assim, com que seja mais fácil encontrar exatamente o que você está procurando. Quanto mais específicas forem as opções de filtro usadas, mais limitados serão os resultados.

O que: - Digite uma cadeia de caracteres (palavra ou parte de uma palavra). Somente os registros que contém essa cadeia de caracteres serão exibidos. O restante dos registros não ficará visível para que seja mais fácil visualizar.

Procurar em colunas: - Selecione quais colunas deverão ser consideradas na filtragem. Você pode marcar uma ou mais colunas para usar na filtragem. Por padrão, todas as colunas são marcadas:

- **Hora**
- **Módulo**
- **Evento**
- **Usuário**

Tipos de objetos: - Permite escolher que tipo de registros exibir. É possível escolher um tipo específico de registro, vários tipos ao mesmo tempo ou exibir todos os tipos de registros (por padrão):

- **Diagnóstico**
- **Informações**
- **Alerta**
- **Erro**
- **Crítico**

Período de tempo: - Use esta opção para filtrar registros por um determinado período de tempo. Você pode escolher um dos seguintes:

- **Log completo** (padrão) – não filtra por período, pois mostra todo o relatório
- **Último dia**
- **Última semana**
- **Último mês**
- **Intervalo** – ao selecionar o intervalo, é possível especificar o período de tempo exato (data e hora) para exibir somente os registros que ocorreram no período de tempo especificado.

Além das configurações de filtragem anteriores, há também várias **Opções**:

Coincidir apenas palavras inteiras – Mostra apenas os registros que correspondam à cadeia de caracteres como uma palavra inteira na caixa de texto **O que**.

Diferenciar maiúsculas de minúsculas – Mostra apenas os registros que correspondam à cadeia de caracteres com maiúsculas e minúsculas exatas na caixa de texto **O que**.

Ativar filtragem inteligente – Use essa opção para que o ESET File Security execute a filtragem usando seus próprios métodos.

Após terminar de escolher as opções de filtragem, pressione o botão **OK** para aplicar o filtro. A janela **Relatórios** exibirá apenas os registros correspondentes de acordo com as opções do filtro.

4.6.2 Localizar no relatório

Além da Filtragem de relatórios, é possível usar o recurso de pesquisa nos relatórios e usá-lo independente da filtragem de relatórios. Isso é útil quando você está procurando registros específicos nos relatórios. Assim como a Filtragem de relatórios, este recurso de pesquisa o ajudará a encontrar as informações que está procurando, especialmente quando há muitos registros.

Ao usar Localizar no relatório, você pode digitar uma cadeia de caracteres com **O que** para encontrar, especificar em quais **colunas procurar**, selecionar os **Tipos de registro** e definir um **Período de tempo** para pesquisar apenas por registros que ocorreram nesse período de tempo. Ao especificar determinadas opções de pesquisa, apenas os registros relevantes (de acordo com as opções de filtro) serão pesquisados na janela Relatórios.

Para pesquisar nos relatórios, abra a janela **Localizar no relatório** pressionando as teclas Ctrl + F.

OBSERVAÇÃO: Você pode usar o recurso Localizar no relatório em conjunto com a Filtragem de relatórios. Pode limitar primeiro a quantidade de registros usando a Filtragem de relatórios e, em seguida, iniciar a pesquisa somente nos registros filtrados.

O que: - Digite uma cadeia de caracteres (palavra ou parte de uma palavra). Somente os registros que contém essa cadeia de caracteres serão localizados. O restante dos registros será omitido.

Procurar em colunas: - Selecione quais colunas deverão ser consideradas na pesquisa. Você pode marcar uma ou mais colunas para usar na pesquisa. Por padrão, todas as colunas estão marcadas:

- **Hora**
- **Módulo**
- **Evento**
- **Usuário**

Tipos de objetos: - Permite escolher que tipo de registros localizar. Você pode escolher um tipo de registro específico, vários tipos ao mesmo tempo ou pesquisar em todos os tipos de registro (por padrão):

- **Diagnóstico**
- **Informações**
- **Alerta**
- **Erro**
- **Crítico**

Período de tempo: - Use esta opção para localizar registros que ocorreram apenas dentro de determinado período de tempo. Você pode escolher um dos seguintes:

- **Log completo** (padrão) – não pesquisa no período de tempo, mas em todo o relatório
- **Último dia**
- **Última semana**
- **Último mês**
- **Intervalo** – ao selecionar o intervalo, é possível especificar o período de tempo exato (data e hora) para pesquisar somente os registros que ocorreram no período de tempo especificado.

Além das configurações de localização anteriores, há também várias **Opções**:

Coincidir apenas palavras inteiras – Localiza apenas os registros que correspondam à cadeia de caracteres como uma palavra inteira na caixa de texto **O que**.

Diferenciar maiúsculas de minúsculas – Localiza apenas os registros que correspondam à cadeia de caracteres com maiúsculas e minúsculas exatas na caixa de texto **O que**.

Pesquisar acima – Pesquisa da posição atual para cima.

Após configurar as opções de pesquisa, clique no botão **Localizar** para iniciar a pesquisa. A pesquisa pára quando encontrar o primeiro registro correspondente. Clique no botão **Localizar** novamente para continuar pesquisando. A pesquisa ocorre de cima para baixo nos Relatórios, començando na posição atual (registro destacado).

4.6.3 Manutenção de relatórios

A configuração de relatórios do ESET File Security pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar na configuração avançada...** > **Ferramentas** > **Relatórios**. Você pode especificar as seguintes opções para relatórios:

- **Excluir registros automaticamente**: As entradas do relatório mais antigas que o número de dias especificado serão automaticamente excluídas

- **Otimizar automaticamente relatórios**: Ativa a desfragmentação automática de relatórios se a porcentagem especificada de relatórios não utilizados foi excedida.

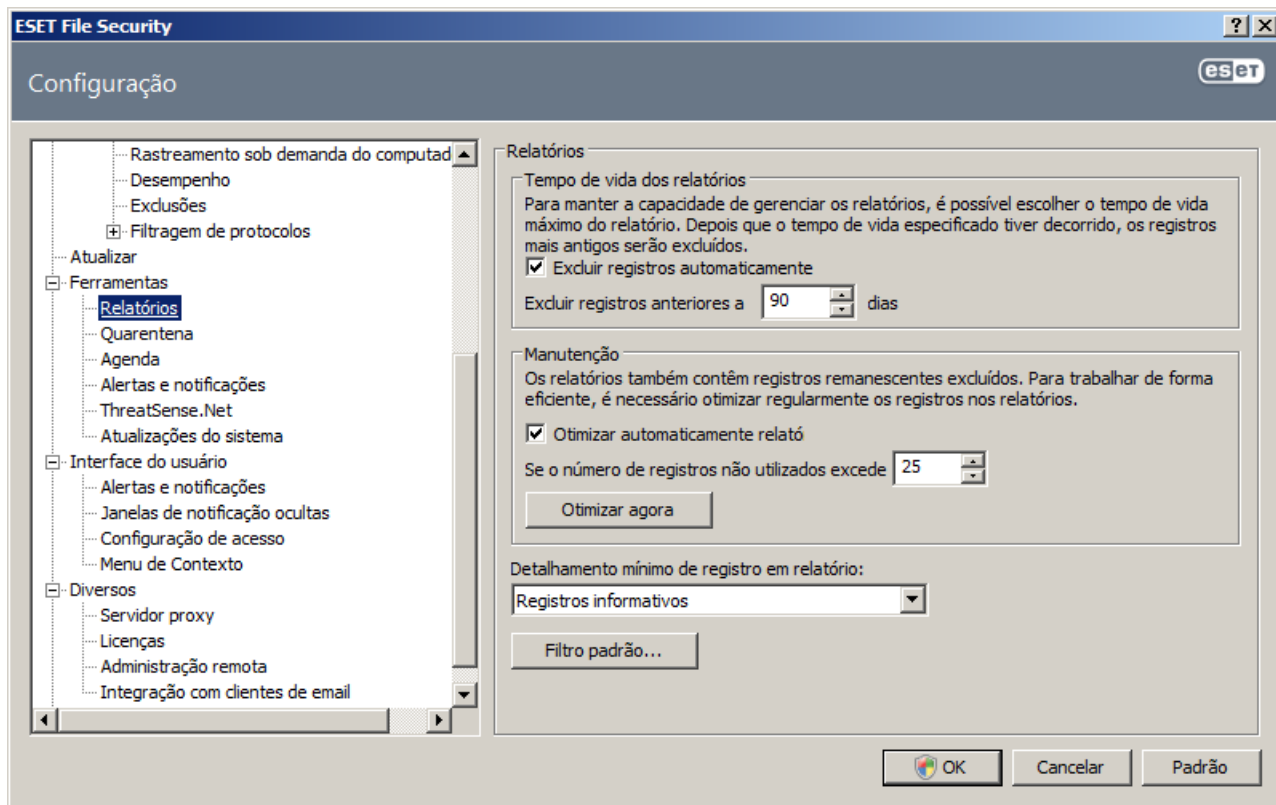
- **Detalhamento mínimo de registro em relatório**: Especifica o nível de detalhamento de registro em relatório. Opções disponíveis:

\- **Registros de diagnóstico** – Registra as informações necessárias para ajustar o programa e todos os registros mencionados anteriormente

\- **Registros informativos** – Registra as mensagens informativas, incluindo atualizações bem-sucedidas e todos os registros mencionados anteriormente

\- **Avisos** – Registra mensagens de erros críticos e de avisos

\- **Erros** – Somente as mensagens do tipo "Erro ao fazer download de arquivo" e erros críticos serão registrados

\- **Avisos críticos** – Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, etc.)

4.7 ESET SysInspector

4.7.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada em soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões são idênticas em função e têm os mesmos controles de programa. A única diferença é como os resultados são gerenciados. As versões integrada e separada permitem exportar snapshots do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os snapshots do sistema diretamente em **Ferramentas** > **ESET SysInspector** (exceto ESET Remote Administrator). Para obter mais informações, consulte a seção ESET SysInspector como parte do ESET File Security.

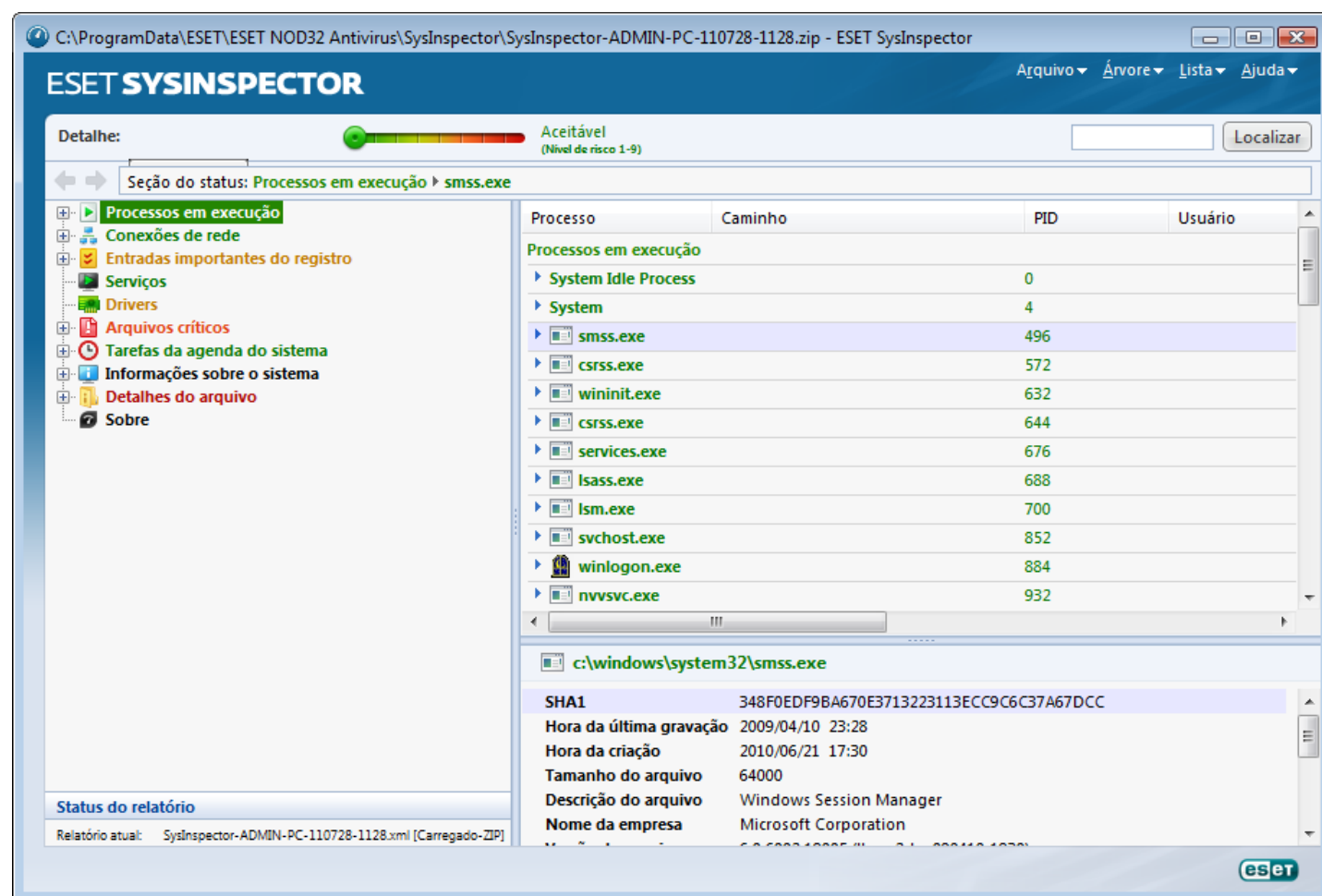
Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

4.7.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo *SysInspector.exe* obtido por download no site da ESET. Se você já tiver uma das soluções ESET Security instalada, poderá executar o ESET SysInspector diretamente do Menu Iniciar (**Programas** > **ESET** > **ESET File Security**).

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos, dependendo do hardware e dos dados a serem coletados.

4.7.2 Interface do usuário e uso do aplicativo

Para facilitar o uso, a janela principal é dividida em quatro seções: Controles do programa, localizados na parte superior da janela principal, a janela de navegação à esquerda, a janela de descrição à direita e no centro, e a janela de detalhes à direita, na parte inferior da janela principal. A seção Status do relatório lista os parâmetros básicos de um relatório (filtro usado, tipo do filtro, se o relatório é resultado de uma comparação, etc.).

4.7.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um relatório armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um relatório **Adequado para envio**. Neste formulário, o relatório omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente simplesmente arrastando e soltando-os na janela principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela principal, para que seja mais fácil trabalhar com estas informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe menos detalhes usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para solucionar problemas muito específicos.

Filtragem de itens

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver totalmente à esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante totalmente à direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens classificados como risco 6 a 9 podem ser um risco à segurança. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrar esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Pesquisar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, verifique se os arquivos são realmente perigosos ou desnecessários.

4.7.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou, como alternativa, clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do relatório. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo e o nível de risco do arquivo.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados 24 horas por dia, 7 dias por semana e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do

arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas frequentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como Serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de tarefas do Windows em um intervalo/horário especificado.

Informações do sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas e direitos do usuário.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista de módulos do programa.

4.7.2.2.1 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O abre o relatório existente
Ctrl+S salva os relatórios criados

Gerar

Ctrl+G gera um instantâneo padrão do status do computador
Ctrl+H gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O aceitável, nível de risco 1-9, os itens são exibidos

2	aceitável, nível de risco 2-9, os itens são exibidos
3	aceitável, nível de risco 3-9, os itens são exibidos
4, U	desconhecido, nível de risco 4-9, os itens são exibidos
5	desconhecido, nível de risco 5-9, os itens são exibidos
6	desconhecido, nível de risco 6-9, os itens são exibidos
7, B	perigoso, nível de risco 7-9, os itens são exibidos
8	perigoso, nível de risco 8-9, os itens são exibidos
9	perigoso, nível de risco 9, os itens são exibidos
-	diminui o nível de risco
+	aumenta o nível de risco
Ctrl+9	modo de filtragem, nível igual ou superior
Ctrl+0	modo de filtragem, somente nível igual

Exibir

Ctrl+5	exibição por fornecedor, todos os fornecedores
Ctrl+6	exibição por fornecedor, somente Microsoft
Ctrl+7	exibição por fornecedor, todos os outros fornecedores
Ctrl+3	exibe detalhes completos
Ctrl+2	exibe detalhes da mídia
Ctrl+1	exibição básica
Backspace	move um passo para trás
Espaço	move um passo para a frente
Ctrl+W	expande a árvore
Ctrl+Q	recolhe a árvore

Outros controles

Ctrl+T	vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	exibe informações básicas sobre um item
Ctrl+A	exibe informações completas sobre um item
Ctrl+C	copia a árvore do item atual
Ctrl+X	copia itens
Ctrl+B	localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	abre a entrada correspondente no editor do registro
Ctrl+Z	copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	alterna para o campo de pesquisa
Ctrl+D	fecha os resultados da pesquisa
Ctrl+E	executa script de serviços

Comparação

Ctrl+Alt+O	abre o relatório original/comparativo
Ctrl+Alt+R	cancela a comparação
Ctrl+Alt+1	exibe todos os itens
Ctrl+Alt+2	exibe apenas os itens adicionados; o relatório mostrará os itens presentes no relatório atual
Ctrl+Alt+3	exibe apenas os itens removidos; o relatório mostrará os itens presentes no relatório anterior
Ctrl+Alt+4	exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	exibe apenas as diferenças entre os relatórios
Ctrl+Alt+C	exibe a comparação
Ctrl+Alt+N	exibe o relatório atual
Ctrl+Alt+P	exibe o relatório anterior

Diversos

F1	exibe a ajuda
Alt+F4	fecha o programa
Alt+Shift+F4	fecha o programa sem perguntar
Ctrl+I	estatísticas de relatórios

4.7.2.3 Comparar

O recurso Comparar permite que o usuário compare dois relatórios existentes. O resultado desse recurso é um conjunto de itens não comuns em ambos os relatórios. Ele é adequado se você deseja manter controle das alterações no sistema; é uma ferramenta útil para detectar a atividade de código malicioso.

Após ser iniciado, o aplicativo criará um novo relatório que será exibido em uma nova janela. Navegue até **Arquivo** > **Salvar relatório** para salvar um relatório em um arquivo. Os relatórios podem ser abertos e visualizados posteriormente. Para abrir um relatório existente, utilize o menu **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um relatório de cada vez.

O benefício de comparar dois relatórios é que você pode visualizar um relatório ativo no momento e um relatório salvo em um arquivo. Para comparar relatórios, utilize a opção **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O relatório selecionado será comparado com o relatório ativo na janela principal do programa. O relatório comparativo exibirá apenas as diferenças entre esses dois relatórios.

OBSERVAÇÃO: Caso compare dois relatórios, selecione **Arquivo** > **Salvar relatório** e salve-o como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir este arquivo posteriormente, os relatórios contidos serão comparados automaticamente.

Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os relatórios comparados.

Os itens marcados por um − apenas podem ser encontrados no relatório ativo e não estavam presentes no relatório comparativo aberto. Os itens marcados por um + estavam presentes apenas no relatório aberto e estavam ausentes no relatório ativo.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- + novo valor, não presente no relatório anterior
- a seção de estrutura em árvore contém novos valores
- − valor removido, presente apenas no relatório anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no relatório anterior
- o nível de risco aumentou / era menor no relatório anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos relatórios que estão sendo comparados.

Qualquer relatório comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois relatórios, navegue até **Arquivo** > **Comparar relatórios**. O programa criará um relatório comparativo mostrando as diferenças entre os relatórios.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

4.7.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar um relatório diretamente a partir da linha de comando sem executar a GUI
/privacy	gerar um relatório excluindo informações confidenciais
/zip	armazenar o relatório resultante diretamente no disco em um arquivo compactado
/silent	ocultar a exibição da barra de progresso da geração de relatórios
/help, /?	exibir informações sobre os parâmetros da linha de comando

Exemplos

Para carregar um relatório específico diretamente no navegador, use: *SysInspector.exe "c:\clientlog.xml"*
Para gerar um relatório em um local atual, use: *SysInspector.exe /gen*
Para gerar um relatório em uma pasta específica, use: *SysInspector.exe /gen="c:\folder\"*
Para gerar um relatório em um arquivo/local específico, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Para gerar um relatório que exclua informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Para comparar dois relatórios, use: *SysInspector.exe "current.xml" "original.xml"*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

4.7.4 Script de serviços

O script de serviços é uma ferramenta que oferece ajuda a clientes que usam o ESET SysInspector, removendo facilmente objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o relatório modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As alterações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador esteja infectado por um vírus que não é detectado pelo seu programa antivírus, siga as instruções passo-a-passo a seguir:

- Execute o ESET SysInspector para gerar um novo snapshot do sistema.
- Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Ctrl e selecione o último item para marcar todos os itens.
- Clique com o botão direito nos objetos selecionados e selecione a opção do menu de contexto **Exportar as seções selecionadas para script de serviços**.
- Os objetos selecionados serão exportados para um novo relatório.
- Esta é a etapa mais crucial de todo o procedimento: abra o novo relatório e altere o atributo – para + para todos os objetos que desejar remover. Certifique-se de não marcar nenhum arquivo/objeto importante do sistema operacional.
- Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o seu script.
- Clique em **OK** para executar o script.

4.7.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector. No menu de contexto, selecione a opção **Exportar todas as seções para script de serviços** ou a opção **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois relatórios estiverem sendo comparados.

4.7.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, há informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do relatório (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup:
Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup:
Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando você executar o script, os drivers selecionados serão interrompidos. Observe que alguns drivers não permitirão eles mesmos a interrupção.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos críticos para o sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos, ou serão restaurados seus valores padrão originais.

4.7.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma caixa de diálogo confirmará que o script foi executado com sucesso.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

4.7.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um relatório?

O ESET SysInspector pode criar um relatório da configuração do computador. Para salvar um relatório, selecione **Arquivo** > **Salvar relatório** no menu principal. Os relatórios são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\My Documents*, com uma convenção de nomenclatura de arquivos de "SysInpsector-%NOMECOMPUTADOR%-AAMMDD-HHMM.XML". Você pode alterar o local e o nome do relatório para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o relatório do ESET SysInspector?

Para visualizar um relatório criado pelo ESET SysInspector, execute o programa e selecione **Arquivo** > **Abrir relatório** no menu principal. Você também pode arrastar e soltar relatórios no aplicativo ESET SysInspector. Se você precisar visualizar os relatórios do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os relatórios para visualização. Por motivo de segurança, os Windows Vista/7 podem não permitir operações de arrastar e soltar entre janelas que tenham permissões de segurança diferentes.

Há uma especificação disponível para o formato do relatório? E um SDK?

Atualmente, não há uma especificação para o relatório nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 - Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro deles.

Um nível de risco "6 – Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles também podem examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporta como um rootkit, o usuário será exposto ao risco de danos ou roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validando usando essas informações. Se uma assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado. Se o arquivo CAT pertinente for encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

Exemplo:

O Windows 2000 inclui o aplicativo HyperTerminal, localizado em *C:\Arquivos de Programas\Windows NT*. O arquivo executável principal do aplicativo não é assinado digitalmente, mas o ESET SysInspector o marca como um arquivo assinado pela Microsoft. O motivo disso é a referência em *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que aponta para *C:\Arquivos de Programas\Windows NT\hypertrm.exe* (o executável principal do aplicativo HyperTerminal) e o *sp4.cat* é digitalmente assinado pela Microsoft.

4.7.6 ESET SysInspector como parte do ESET File Security

Para abrir a seção do ESET SysInspector no ESET File Security, clique em **Ferramentas** > **ESET SysInspector**. O sistema de gerenciamento na janela do ESET SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com snapshots: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do ESET SysInspector contém informações básicas sobre os snapshots criados, como a hora da criação, breve comentário, nome do usuário que criou o snapshot e o status do snapshot.

Para comparar, criar... ou excluir snapshots, utilize os botões correspondentes localizados abaixo da lista de snapshots na janela do ESET SysInspector. Essas opções também estão disponíveis no menu de contexto. Para exibir o snapshot do sistema selecionado, utilize a opção do menu de contexto **Exibir**. Para exportar o snapshot selecionado para um arquivo, clique com o botão direito e selecione **Exportar...**.

Abaixo, há uma descrição detalhada das opções disponíveis:

- **Comparar** – permite comparar dois relatórios existentes. Ela é adequada se você desejar controlar alterações entre o relatório atual e um relatório anterior. Para que essa opção entre em vigor, é necessário selecionar dois snapshots a serem comparados.
- **Criar...** - Cria um novo registro. Antes disso, é preciso inserir um breve comentário sobre o registro. Para localizar o progresso de criação do snapshot (do snapshot gerado no momento), veja a coluna **Status**. Todos os snapshots concluídos são marcados com o status **Criado**.
- **Excluir/Excluir tudo** - Remove as entradas da lista.
- **Exportar...** - Salva a entrada selecionada em um arquivo XML (também em uma versão compactada).

4.8 ESET SysRescue

ESET SysRescue é um utilitário que permite criar um disco inicializável que contém uma das soluções ESET Security - pode ser o ESET NOD32 Antivirus, ESET Smart Security ou até mesmo alguns dos produtos orientados a servidor. A principal vantagem do ESET SysRescue é o fato de que a solução ESET Security é executada de maneira independente do sistema operacional host, ao mesmo tempo em que possui um acesso direto ao disco e a todo o sistema de arquivos. Isso possibilita remover as infiltrações que normalmente não poderiam ser excluídas, por exemplo, quando o sistema operacional está em execução, etc.

4.8.1 Requisitos mínimos

O ESET SysRescue funciona no Microsoft Windows Preinstallation Environment (Windows PE) versão 2.x, que é baseado no Windows Vista.

O Windows PE faz parte dos pacotes gratuito do Windows Automated Installation Kit (Windows AIK) ou Windows Assessment and Deployment Kit (Windows ADK), portanto o Windows AIK ou ADK deve ser instalado antes da criação do ESET SysRescue (http://go.eset.eu/AIK) ou (http://go.eset.eu/ADK). Qual desses kits deverá ser instalado em seu sistema dependerá da versão do sistema operacional que você está executando. Devido ao suporte da versão de 32 bits do Windows PE, é necessário usar o pacote de instalação de 32 bits da solução ESET Security ao criar o ESET SysRescue em sistemas de 64 bits. O ESET SysRescue é compatível com o Windows AIK 1.1 e posteriores, bem como com o Windows ADK.

OBSERVAÇÃO: Como o Windows AIK tem mais de 1 GB em tamanho e o Windows ADK tem 1,3 GB em tamanho, é necessária uma conexão com a internet de alta velocidade para um download perfeito.

O ESET SysRescue está disponível em soluções ESET Security versão 4.0 e posteriores.

O ESET SysRescue écompatível com os seguintes sistemas operacionais:

- Windows Server 2003 Service Pack 1 com KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

O Windows AIK é compatível com:

- Windows Server 2003
- Windows Server 2008

O Windows ADK é compatível com:

- Windows Server 2012

4.8.2 Como criar o CD de restauração

Para iniciar o assistente do ESET SysRescue, clique em **Iniciar** > **Programas** > **ESET** > **ESET File Security** > **ESET SysRescue**.

Primeiro, o assistente verifica a presença do Windows AIK ou ADK e de um dispositivo adequado para a criação da mídia de inicialização. Se o Windows AIK ou Windows ADK não estiver instalado no computador (ou estiver corrompido ou instalado incorretamente), o assistente dará a opção de instalá-lo ou de inserir o caminho para a pasta do Windows AIK (http://go.eset.eu/AIK) ou Windows ADK (http://go.eset.eu/ADK).

OBSERVAÇÃO: Como o Windows AIK tem mais de 1 GB em tamanho e o Windows ADK tem 1,3 GB em tamanho, é necessária uma conexão com a internet de alta velocidade para um download perfeito.

Na próxima etapa, selecione a mídia de destino em que o ESET SysRescue estará localizado.

4.8.3 Seleção de alvos

Além de CD/DVD/USB, você pode escolher salvar o ESET SysRescue em um arquivo ISO. Posteriormente, é possível gravar a imagem ISO em CD/DVD ou utilizá-la de alguma outra maneira (por exemplo, no ambiente virtual, como VMWare ou VirtualBox).

Se você selecionar USB como a mídia-alvo, a reinicialização pode não funcionar em determinados computadores. Algumas versões de BIOS podem relatar problemas com o BIOS – comunicação com o gerenciador de inicialização (por exemplo, no Windows Vista), e a inicialização é encerrada com a seguinte mensagem de erro:

```
arquivo: \boot\bcd
status: 0xc000000e
informações: an error occurred while attemping to read the boot configuration data (ocorreu um erro ao tentar ler os d
```

Se você encontrar essa mensagem, recomendamos selecionar o CD, em vez da mídia USB.

4.8.4 Configurações

Antes de iniciar a criação do ESET SysRescue, o assistente de instalação exibirá os parâmetros de compilação na última etapa do assistente do ESET SysRescue. Esses parâmetros podem ser alterados clicando no botão **Alterar...**. As opções disponíveis incluem:

- Pastas
- Antivírus ESET
- Avançado
- Protoc. Internet
- Dispositivo USB inicializável (quando o dispositivo USB de destino estiver selecionado)
- Gravação (quando a unidade de CD/DVD de destino estiver selecionada)

O botão **Criar** estará inativo se nenhum pacote de instalação MSI for especificado ou se nenhuma solução ESET Security estiver instalada no computador. Para selecionar um pacote de instalação, clique no botão **Alterar** e vá para a guia **Antivírus ESET**. Além disso, se você não preencher o nome de usuário e a senha (**Alterar** > **Antivírus ESET**), o botão **Criar** estará acinzentado.

4.8.4.1 Pastas

A **Pasta temporária** é um diretório de trabalho para arquivos exigidos durante a compilação do ESET SysRescue.

Pasta ISO é uma pasta, em que o arquivo ISO resultante é salvo após a conclusão da compilação.

A lista nessa guia mostra todas as unidades de rede locais e mapeadas, junto com o espaço livre disponível. Se algumas das pastas aqui estão localizadas em uma unidade com espaço livre insuficiente, recomendamos que você selecione outra unidade com mais espaço livre disponível. Caso contrário, a compilação pode ser encerrada prematuramente devido a espaço livre em disco insuficiente.

Aplicativos externos - Permite especificar os programas adicionais que serão executados ou instalados após a inicialização a partir de uma mídia do ESET SysRescue.

Incluir aplicativos externos - Permite adicionar programas externos à compilação do ESET SysRescue.

Pasta selecionada - Pasta na qual os programas a serem adicionados ao disco do ESET SysRescue estão localizados.

4.8.4.2 Antivírus ESET

Para criação do CD do ESET SysRescue, é possível selecionar duas fontes de arquivos da ESET para serem utilizadas pelo compilador.

Pasta ESS/EAV - Arquivos já contidos na pasta na qual a solução ESET Security está instalada no computador.

Arquivo MSI - Os arquivos contidos no instalador do MSI são usados.

A seguir, você pode escolher atualizar o local dos arquivos (.nup). Geralmente, a opção padrão **Pasta ESS/EAV/ Arquivo MSI** está definida. Em alguns casos, uma **Pasta atualiz** personalizada pode ser escolhida, p.ex., para usar uma versão mais recente ou mais antiga do banco de dados de assinatura de vírus.

É possível utilizar uma das seguintes fontes de nome de usuário e senha:

ESS/EAV instalado - O nome de usuário e a senha são copiados da solução ESET Security instalada no momento.

Do usuário - O nome de usuário e a senha digitados nas caixas de texto correspondentes serão utilizados.

OBSERVAÇÃO: O ESET Security no CD do ESET SysRescue é atualizado na Internet ou na solução ESET Security instalada no computador em que o CD do ESET SysRescue for executado.

4.8.4.3 Configurações avançadas

A guia **Avançado** permite otimizar o CD do ESET SysRescue de acordo com o tamanho da memória do computador. Selecione **576 MB ou mais** para gravar o conteúdo do CD na memória operacional (RAM). Se você selecionar **menos de 576 MB**, o CD de recuperação será permanentemente acessado quando o WinPE estiver em execução.

Na seção **Drivers externos**, é possível inserir drivers para o seu hardware específico (geralmente adaptador de rede). Embora o WinPE seja baseado no Windows Vista SP1, que suporta hardware de larga escala, algumas vezes o hardware não é reconhecido. Isso requer que o driver seja adicionado manualmente. Há duas maneiras de inserir o driver em uma compilação do ESET SysRescue – manualmente (botão **Adicionar**) e automaticamente (botão **Pesquisa auto**). No caso de inclusão manual, é preciso selecionar o caminho para o arquivo .inf correspondente (o arquivo *.sys aplicável também deve estar presente nessa pasta). No caso de inserção automática, o driver é encontrado automaticamente no sistema operacional do computador específico. Recomendamos usar a inclusão automática apenas se o ESET SysRescue for usado em um computador com o mesmo adaptador de rede usado no computador em que o CD do ESET SysRescue foi criado. Durante a criação, o driver do ESET SysRescue é inserido na compilação para que você não precise procurá-lo depois.

4.8.4.4 Protocolo da Internet

Esta seção permite configurar as informações básicas de rede e as conexões predefinidas após o ESET SysRescue.

Selecione **Endereço IP privado autom.** para obter o endereço IP automaticamente do servidor DHCP (Dynamic Host Configuration Protocol).

Alternativamente, esta conexão de rede pode usar um endereço IP especificado manualmente (também conhecido como IP estático). Selecione **Personalizado** para configurar os ajustes de IP correspondentes. Se selecionar esta opção, é necessário especificar um **Endereço IP** e, para conexões de rede e de banda larga, uma **Másc subrede**. Em **Serv. DNS prefer.** e **Serv. DNS altern.**, digite os endereços dos servidores de DNS primário e secundário.

4.8.4.5 Dispositivo USB inicializável

Se você selecionou o dispositivo USB como mídia de destino, é possível selecionar uma das mídias USB disponíveis na guia **Dispositivo USB inicializável** (caso haja mais dispositivos USB).

Selecione o **Dispositivo** alvo apropriado em que o ESET SysRescue será instalado.

Alerta: O dispositivo USB selecionado será formatado durante o processo de criação do ESET SysRescue. Todos os dados no dispositivo serão excluídos.

Se escolher a opção **Formato rápido**, a formatação remove todos os arquivos da partição, mas não procura setores corrompidos no disco. Use esta opção se seu dispositivo USB tiver sido formatado anteriormente e você tiver certeza de que não está danificado.

4.8.4.6 Gravar

Se você selecionou CD/DVD como sua mídia-alvo, é possível especificar parâmetros de gravação adicionais na guia **Gravar**.

Excluir arquivo ISO - Marque essa opção para excluir o arquivo ISO temporário após o CD do ESET SysRescue ser criado.

Exclusão ativada - Permite selecionar o apagamento rápido e concluí-lo.

Dispositivo de gravação - Selecione a unidade a ser utilizada para gravação.

Aviso: Essa é a opção padrão. Se um CD/DVD regravável for usado, todos os dados contidos no CD/DVD serão apagados.

A seção Mídia contém informações sobre a mídia no seu dispositivo de CD/DVD.

Velocidade de gravação - Selecione a velocidade desejada no menu suspenso. Os recursos do seu dispositivo de gravação e o tipo de CD/DVD utilizado devem ser considerados na seleção da velocidade da gravação.

4.8.5 Trabalhar com o ESET SysRescue

Para o CD/DVD/USB de restauração funcionar de forma eficiente, é necessário que o computador seja inicializado a partir da mídia de inicialização do ESET SysRescue. A prioridade de inicialização pode ser modificada no BIOS. Como alternativa, você pode usar o menu de inicialização durante a inicialização do computador, geralmente utilizando uma das teclas F9 ou F12, dependendo da versão da placa-mãe/do BIOS.

Após a inicialização da mídia, a solução ESET Security será iniciada. Como o ESET SysRescue é utilizado apenas em situações específicas, alguns módulos de proteção e recursos do programa presentes na versão padrão da solução ESET Security não são necessários; a lista é limitada ao **Rastreamento do computador**, **Atualizar** e algumas seções na **Configuração**. A capacidade de atualizar o banco de dados de assinaturas de vírus é o recurso mais importante do ESET SysRescue. Recomendamos que você atualize o programa antes de iniciar um rastreamento do computador.

4.8.5.1 Utilização do ESET SysRescue

Suponha que os computadores na rede tenham sido infectados por um vírus que modifica os arquivos executáveis (.exe). A solução ESET Security é capaz de limpar todos os arquivos infectados, exceto *explorer.exe*, que não pode ser limpo, mesmo no modo de segurança. Isso ocorre porque o *explorer.exe*, como um dos processos essenciais do Windows, também é iniciado no modo de segurança. A solução ESET Security não poderia realizar ações com o arquivo e ele permaneceria infectado.

Nesse tipo de cenário, seria possível usar o ESET SysRescue para solucionar o problema. O ESET SysRescue não requer componentes do sistema operacional host, portanto ele pode processar (limpar, excluir) qualquer arquivo no disco.

4.9 Interface do usuário

As opções de configuração da interface do usuário no ESET File Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário** da árvore Configuração avançada do ESET File Security.

Na seção **Elementos da interface do usuário**, a opção **Modo avançado** proporciona aos usuários a capacidade de alternar para o Modo avançado. O Modo avançado exibe as configurações mais detalhadas e os controles adicionais do ESET File Security.

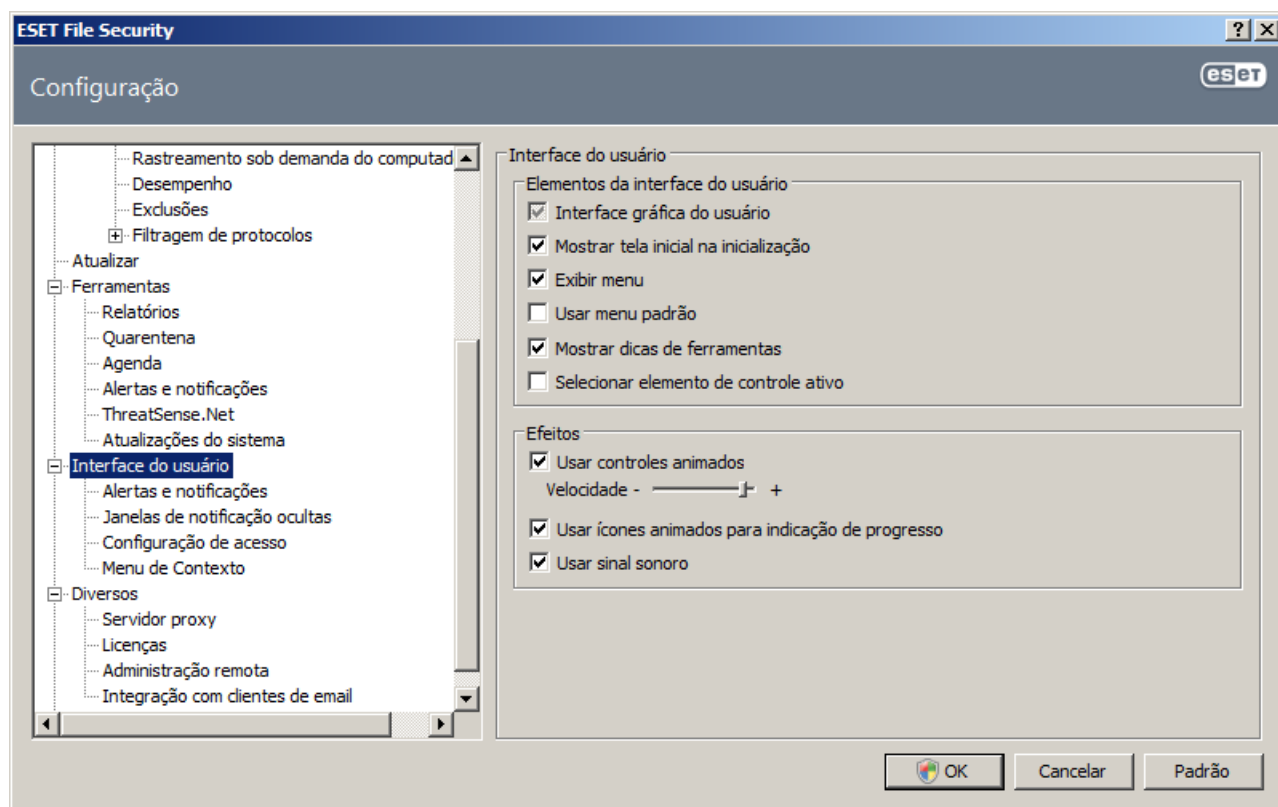
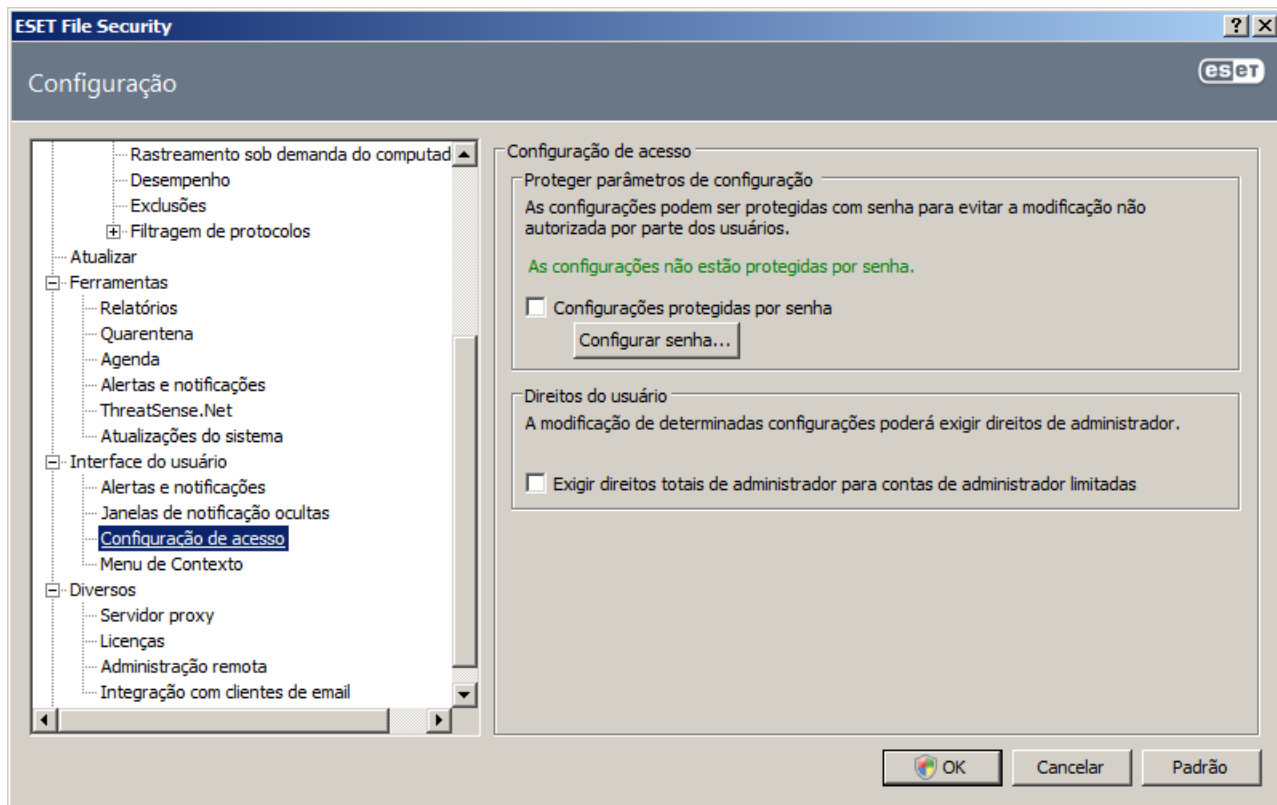
A opção **Interface gráfica do usuário** deve ser desativada se os elementos gráficos reduzirem o desempenho do computador ou provocarem outros problemas. A interface gráfica também pode precisar ser desativada para usuários com deficiência visual, uma vez que pode causar conflito com aplicativos especiais usados para leitura do texto exibido na tela.

Se desejar desativar a tela inicial do ESET File Security, desmarque a opção **Mostrar tela inicial na inicialização**.

No parte superior da janela principal do tela do ESET File Security, há um menu padrão que pode ser ativado ou desativado com base na opção **Usar menu padrão**.

Se a opção **Mostrar dicas de ferramentas**, uma descrição breve será exibida se o cursor for colocado em cima da opção. A opção **Selecionar elemento de controle ativo** fará com que o sistema destaque qualquer elemento que esteja atualmente na área ativa do cursor do mouse. O elemento realçado será ativado após um clique no mouse.

Para diminuir ou aumentar a velocidade dos efeitos animados, selecione a opção **Usar controles animados** e mova a barra deslizante **Velocidade** para a esquerda ou para a direita.

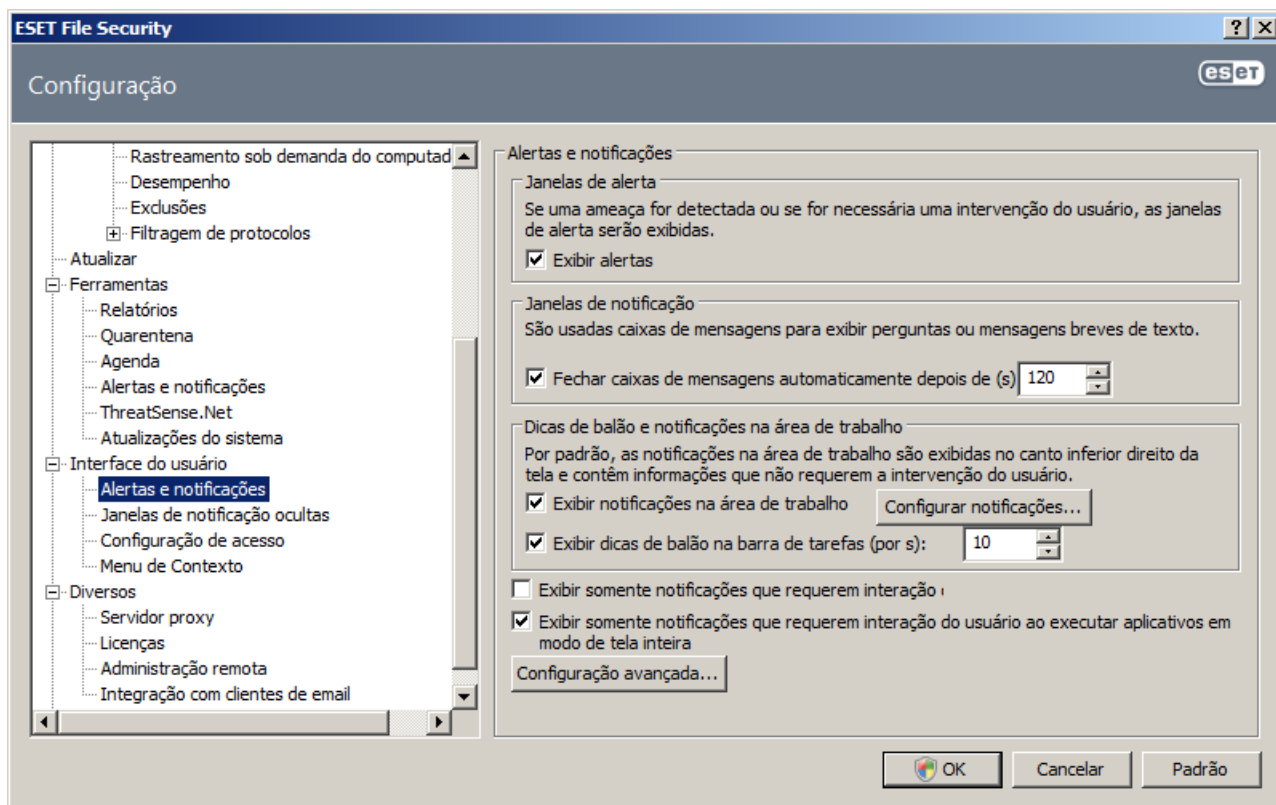
Para ativar o uso de ícones animados para exibir o andamento de várias operações, selecione a opção **Usar ícones animados para indicação de progresso**. Se desejar que o programa emita um aviso sonoro se um evento importante ocorrer, selecione a opção **Usar sinal sonoro**.

O recurso **Interface do usuário** também inclui a opção de proteger por senha os parâmetros de configuração do ESET File Security. Essa opção está localizada no submenu **Proteção de configurações** em **Interface do usuário**. Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. Modificações não autorizadas podem resultar na perda de dados importantes. Para definir uma senha para proteger os parâmetros de configuração, clique em **Configurar senha...**

4.9.1 Alertas e notificações

A seção **Configuração de alertas e notificações** em **Interface do usuário** permite que você configure o modo como os alertas de ameaças e as notificações do sistema são tratados no ESET File Security.

O primeiro item é **Exibir alertas**. A desativação dessa opção cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente depois de (s)**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente depois de expirado o tempo especificado.

As notificações na área de trabalho e as dicas de balão são apenas informativas e não requerem nem proporcionam interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar a exibição de notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas - o tempo de exibição e a transparência da janela de notificação podem ser modificados clicando no botão **Configurar notificações...**

Para visualizar o comportamento das notificações, clique no botão **Visualizar**. Para configurar a duração da exibição das dicas de balão, consulte a opção **Exibir dicas de balão na barra de tarefas (por s)**.

Clique em **Configuração avançada...** para inserir opções de configuração de **Alertas e notificações** adicionais que incluem **Exibir somente notificações que requerem interação do usuário**. Essa opção permite ativar/desativar a exibição de alertas e notificações que não requeiram interação do usuário. Selecione **Exibir somente notificações que requerem interação do usuário ao executar aplicativos em modo de tela inteira** para suprimir todas as notificações que não sejam interativas. No menu suspenso **Detalhamento mínimo de eventos para exibir**, é possível selecionar o nível de gravidade inicial dos alertas e das notificações a serem exibidos.

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário**: permite definir quem receberá notificações importantes do ESET File Security. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Essa opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

4.9.2 Desativar a GUI no servidor de terminal

Este capítulo descreve como desativar a GUI do ESET File Security em execução no servidor de terminal do Windows para sessões de usuário.

Normalmente, a GUI do ESET File Security é iniciada toda vez que um usuário remoto faz login no servidor e cria uma sessão de terminal. Isso geralmente é indesejável em servidores de terminal. Se desejar desativar a GUI para sessões de terminal, siga estas etapas:

1. Execute *regedit.exe*
2. Navegue até *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Clique com o botão direito do mouse no Valor *egui* e selecione *Modificar...*
4. Adicione uma alternância de comando `/terminal` ao fim da cadeia de caracteres existente

Veja um exemplo de como devem ser os dados do Valor de *egui* :

```
"C:\Arquivos de Programas\ESET\ESET File Security\egui.exe" /hide /waitservice /terminal
```

Se desejar reverter essa configuração e ativar a inicialização automática da GUI do ESET File Security, remova a alternância `/terminal` Para acessar o Valor do registro *egui*, repita as etapas de 1. a 3.

4.10 eShell

O eShell (abreviação de ESET Shell) é a interface de linha de comando do ESET File Security. É uma alternativa à interface gráfica do usuário (GUI). O eShell possui todos os recursos e opções que a GUI geralmente oferece. O eShell permite configurar e administrar todo o programa sem usar a GUI.

Além de todas as funções e recursos disponíveis na GUI, o eShell também oferece a possibilidade de obter automação executando scripts para configurar, alterar configurações ou realizar uma ação. O eShell também pode ser útil para quem prefere usar linhas de comando em vez da GUI.

Esta seção explica como navegar e como usar o eShell, e lista todos os comandos com uma descrição da função de cada comando específico.

Há dois modos em que o eShell pode ser executado:

- Modo interativo: útil quando se deseja trabalhar com o eShell (não apenas executar um único comando), por exemplo para tarefas como alterar a configuração, visualizar relatórios, etc. Também é possível usar o modo interativo se ainda não estiver familiarizado com todos os comandos. O modo interativo facilita a navegação pelo eShell. Também exibe os comandos disponíveis que podem ser usados em este contexto específico.
- Comando único/Modo de lote: use este modo se deseja apenas executar um comando, sem entrar no modo interativo do eShell. Isso pode ser feito no prompt de comando do Windows, digitando `eshell` com os parâmetros apropriados. Por exemplo:

```
eshell set av document status enabled
```

OBSERVAÇÃO: Para executar comandos do eShell no prompt de comando do Windows ou para executar arquivos em lote, é preciso ativar essa função primeiro (o comando `set general access batch always` precisa ser executado no modo interativo). Para obter mais informações sobre o comando set batch, clique aqui.

Para entrar no modo interativo do eShell, você pode usar um dos seguintes dois métodos:

- No menu Iniciar do Windows: **Iniciar** > **Todos os programas** > **ESET** > **ESET File Security** > **ESET shell**
- No prompt de comando do Windows, digite `eshell` e pressione a tecla Enter

Ao executar o eShell no modo interativo pela primeira vez, será exibida uma tela de primeira execução.

```
ESET Shell
ESET Shell 1.0
Copyright (c) 1992-2012 ESET, spol. s r. o. Todos os direitos reservados.
--------------------------------------------------------------------------------
Primeira execuçao
Para exibir esta informaçao novamente, digite:
        guide      /?        -help

Sintaxe:
        [<prefixo>] [<caminho do comando>]  <comando> [<argumentos>]

Por exemplo, para ativar a proteçao do documento, insira:
            set          av document        status      enabled

Operaçao
O comando pode ou nao ser compatível com qualquer das operaçoes. As operaçoes
alteram o significado do comando. Por exemplo, get av status retorna o status
da proteçao ntivírus, enquanto set av status enabled ativa a proteçao
antivírus. Um exemplo de um comando sem prefixo é exit.

As seguintes operaçoes estao disponíveis:
        get             set             select          add             remove
        clear           start           stop            pause           resume
        restore         send            import          export

-- Mais -- <ENTER - Linha, BARRA DE ESPAÇOS - Página, X - Fim>
```

Ela exibe alguns exemplos básicos de como usar o eShell com Sintaxe, Prefixo, Caminho de comando, Formas abreviadas, Aliases, etc. Basicamente, é um guia rápido do eShell.

OBSERVAÇÃO: Se quiser exibir esta tela no futuro, digite o comando `guide` .

OBSERVAÇÃO: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

4.10.1 Uso

Sintaxe
Os comandos devem ser formatados na sintaxe correta para que funcionem e podem ser compostos de um prefixo, contexto, argumentos, opções, etc. Esta é a sintaxe geral utilizada em todo o eShell:

[<prefixo>] [<caminho de comando>] <comando> [<argumentos>]

Exemplo (isto ativa a proteção de documentos):
`SET AV DOCUMENT STATUS ENABLED`

`SET` - um prefixo
`AV DOCUMENT` - caminho para um comando específico, um contexto a que este comando pertence
`STATUS` - o comando em si
`ENABLED` - um argumento para o comando

Ao usar `HELP` ou `?` com um comando, você verá a sintaxe para aquele comando específico. Por exemplo, o prefixo `CLEANLEVEL HELP` exibirá a sintaxe do comando `CLEANLEVEL` :

SINTAXE:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

Observe que `[get]` está entre colchetes. Isso é o que denomina o prefixo `get` como padrão para o comando `cleanlevel` . Isso significa que, ao executar o comando `cleanlevel` sem especificar nenhum prefixo, será usado o prefixo padrão (que neste caso é `get cleanlevel`). Use comandos sem prefixos para economizar tempo ao digitar. Normalmente, `get` é o padrão para a maioria dos comandos, mas é necessário certificar-se qual é o prefixo padrão para um comando específico, e se é exatamente aquele que deseja executar.

OBSERVAÇÃO: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

Prefixo/Operação
Um prefixo é uma operação. O comando `GET` fornecerá a informação de como um determinado recurso do ESET File Security está configurado ou exibirá um status (como `GET AV STATUS` exibirá o status de proteção atual). O comando `SET` configurará o recurso ou alterará seu status (`SET AV STATUS ENABLED` ativará a proteção).

Estes são os prefixos que o eShell permite que você use. Um comando pode ou não ser compatível com qualquer um dos prefixos:

`GET` - retorna as configurações/status atuais
`SET` - define o valor/status
`SELECT` - seleciona um item
`ADD` - adiciona um item
`REMOVE` - remove um item
`CLEAR` - remove todos os itens/arquivos
`START` - inicia uma ação
`STOP` - interrompe uma ação
`PAUSE` - pausa uma ação
`RESUME` - retoma uma ação
`RESTORE` - restaura as configurações/objeto/arquivo padrão
`SEND` - envia um objeto/arquivo
`IMPORT` - importa de um arquivo
`EXPORT` - exporta para um arquivo

Prefixos como `GET` e `SET` são usados com vários comandos, mas alguns comandos, como `EXIT`, não usam prefixos.

Caminho de comando/Contexto
Os comandos são colocados em contextos que formam uma estrutura de árvore. O nível superior da árvore é a raiz. Ao executar o eShell, você está no nível raiz:

```
eShell>
```

Você pode executar o comando a partir daqui ou entrar um nome de contexto para navegar dentro da árvore. Por exemplo, ao entrar no contexto `TOOLS` , ele listará todos os comandos e subcontextos disponíveis ali.

```
ESET Shell
eShell>av
GET ANTISTEALTH      SET ANTISTEALTH      RESTORE ANTISTEALTH
GET CLEANLEVEL       SET CLEANLEVEL       RESTORE CLEANLEVEL
DOCUMENT             EMAIL                GET EXCLUSIONS
ADD EXCLUSIONS       REMOVE EXCLUSIONS    CLEAR EXCLUSIONS
GET EXTENSIONS       ADD EXTENSIONS       REMOVE EXTENSIONS
RESTORE EXTENSIONS   LIMITS               NETFILTER
OBJECTS              OPTIONS              OTHER
REALTIME             GET SELFDEFENSE      SET SELFDEFENSE
RESTORE SELFDEFENSE  GET STATUS           SET STATUS
RESTORE STATUS       WEB

eShell av>_
```

Os que estão em amarelo são comandos que podem ser executados, os que estão em cinza são subcontextos nos quais você pode entrar. Um sub-contexto contém outros comandos.

Se precisar voltar para um nível superior, use `..` (dois pontos). Por exemplo, se estiver em:

`eShell av options>`

digite `..` e você será levado um nível acima para:

`eShell av>`

Se quiser voltar à raiz de `eShell av options>` (que é dois níveis abaixo da raiz), digite apenas `.. ..` (dois pontos e dois pontos separados por espaço). Fazendo isso, você subirá dois níveis, que neste caso é a raiz. Você pode usar este método também quando estiver ainda mais profundo na árvore de contexto. Use a quantidade adequada de `..` para chegar ao nível desejado.

O caminho é relativo ao contexto atual. Se o comando estiver no contexto atual, não insira um caminho. Por exemplo, para executar `GET AV STATUS` digite:

`GET AV STATUS` - se estiver no contexto raiz (a linha de comando exibe `eShell>`)
`GET STATUS` - se estiver no contexto `AV` (a linha de comando exibe `eShell av>`)
`.. GET STATUS` - se estiver no contexto `AV OPTIONS` (a linha de comando exibe `eShell av options>`)

Argumento

Um argumento é uma ação realizada em um comando específico. Por exemplo, o comando `CLEANLEVEL` pode ser usado com os seguintes argumentos:

`none` - Não limpar
`normal` - Limpeza padrão
`strict` - Limpeza rígida

Outro exemplo são os argumentos `ENABLED` ou `DISABLED`, que são usados para ativar ou desativar determinados recursos.

Forma abreviada/Comandos encurtados

O eShell possibilita encurtar contextos, comandos e argumentos (desde que o argumento seja um alternador ou uma opção alternativa). Não é possível encurtar um prefixo ou um argumento que seja um valor concreto, como um número, nome ou caminho.

Exemplos de forma abreviada:

`set status enabled` => `set stat en`
`add av exclusions C:\caminho\arquivo.ext` => `add av exc C:\caminho\arquivo.ext`

Se houver dois comandos ou contextos começando com as mesmas letras, por exemplo ABOUT e AV, e você digitar A como comando abreviado, o eShell não conseguirá decidir qual comando você deseja executar. Será exibida uma mensagem de erro e uma lista de comandos começando com "A" que poderão ser utilizados:

```
eShell>a
O seguinte comando não é exclusivo: a

Os seguintes comandos estão disponíveis neste contexto:
 ABOUT - Exibe informações sobre o programa
 AV - Alterações ao contexto av
```

Adicionar uma ou mais letras (p. ex., AB em vez de apenas A) o eShell executará o comando ABOUT , já que este é o único com estas letras.

OBSERVAÇÃO: Quando quiser ter certeza de que um comando será executado exatamente como deseja, recomendamos que não abrevie comandos, argumentos, etc. e use a forma completa. Dessa forma o comando será executado exatamente como deseja e isso evita erros indesejados. Especialmente no caso de arquivos/scripts em lote.

Aliases

Um alias é um nome alternativo que pode ser usado para executar um comando (desde que o comando tenha um alias atribuído a ele). Há alguns aliases padrão:

(global) help - ?
(global) close - sair
(global) quit - sair
(global) bye - sair
warnlog - eventos de registro das ferramentas
virlog - detecções de registro das ferramentas

"(global)" significa que o comando pode ser usado em qualquer lugar, independente do contexto atual. Um comando pode ter vários aliases atribuídos a ele, por exemplo o comando EXIT tem os aliases CLOSE, QUIT e BYE. Quando quiser sair do eShell, pode usar o comando EXIT ou qualquer um de seus aliases. VIRLOG é um alias para o comando DETECTIONS , que está localizado no contexto TOOLS LOG . Portanto, as detecções do comando estão disponíveis no contexto ROOT , e são mais fáceis de acessar (não é necessário entrar nos contextos TOOLS e LOG , pode executá-lo diretamente de ROOT).

O eShell permite definir seus próprios aliases.

Comandos protegidos

Alguns comandos estão protegidos e só podem ser executados após inserir uma senha.

Guia

Ao executar o comando GUIDE , será exibida uma tela explicando como usar o eShell. Esse comando está disponível no contexto ROOT (eShell>).

Ajuda

Quando o comando HELP for usado sozinho, listará todos os comandos disponíveis com prefixos e subcontextos dentro do contexto atual. Também fornecerá uma breve descrição para cada comando/subcontexto. Ao usar HELP como um argumento com um comando específico (p.ex. CLEANLEVEL HELP), serão exibidos os detalhes para aquele comando. Serão exibidos a SINTAXE, as OPERAÇÕES, os ARGUMENTOS e os ALIASES para o comando com uma breve descrição de cada.

Histórico de comandos

O eShell mantém um histórico dos comandos executados anteriormente. Isso se aplica apenas à sessão interativa atual do eShell. Quando você sair do eShell, o histórico do comando será removido. Use as teclas de seta para cima e para baixo em seu teclado para navegar pelo histórico. Quando encontrar o comando que está procurando, pode executá-lo ou alterá-lo sem ter que digitar todo o comando desde o início.

CLS/Limpar tela

O comando CLS pode ser usado para limpar a tela. Ele funciona da mesma forma que no prompt de comando do Windows ou interface de linha de comando similar.

EXIT/CLOSE/QUIT/BYE

Para fechar ou sair do eShell, você pode usar qualquer desses comandos (EXIT, CLOSE, QUIT ou BYE).

4.10.2 Comandos

Esta seção lista todos os comandos do eShell disponíveis, com sua respectiva descrição.

OBSERVAÇÃO: Os comandos não diferenciam letras maiúsculas e minúsculas, você pode usar qualquer uma e o comando será executado.

Comandos do contexto **ROOT**:

ABOUT

Lista informações sobre o programa. Exibe o nome do produto instalado, o número da versão, os componentes instalados (incluindo número de versão de cada componente) e as informaçoes básicas sobre o servidor e o sistema operacional em que o ESET File Security está sendo executado.

CAMINHO DO CONTEXTO:

```
raiz
```

BATCH

Inicia o modo de lote do eShell. Isto é muito útil ao executar arquivos/scripts em lote e recomendamos usá-lo com arquivos em lote. Coloque `START BATCH` como o primeiro comando no arquivo de lote ou script para ativar o modo de lote. Ao ativar esta função, não será solicitado nada (p.ex. inserção de senha) e os argumentos faltantes serão substituídos pelos padrões. Isso garante que o arquivo em lote não pare no meio porque o eShell está esperando o usuário fazer algo. Dessa forma, o arquivo em lote será executado sem paradas (a menos que haja um erro ou que os comandos no arquivo em lote estejam incorretos).

CAMINHO DO CONTEXTO:

```
raiz
```

SINTAXE:

```
[start] batch
```

OPERAÇÕES:

`start` - Inicia o eShell no modo de lote

CAMINHO DO CONTEXTO:

```
raiz
```

EXEMPLOS:

`start batch` - Inicia o modo de lote do eShell

GUIDE

Exibe a tela da primeira execução.

CAMINHO DO CONTEXTO:

```
raiz
```

SENHA

Geralmente, para executar comandos protegidos por senha você é solicitado uma senha por motivos de segurança. Isso se aplica a comandos como os que desativam a proteção antivírus e os que podem afetar os recursos do ESET File Security. Será solicitada uma senha sempre que executar um desses comandos. Para evitar inserir uma senha a cada vez, você pode definir esta senha. Ela será lembrada pelo eShell e será usada automaticamente quando um comando protegido por senha for executado. Isso significa que não será preciso inseri-la.

OBSERVAÇÃO: A senha definida funciona somente na sessão interativa atual do eShell. Quando você sair do eShell, esta senha definida será removida. Ao iniciar o eShell novamente, a senha precisará ser definida novamente.

Essa senha definida também é bastante útil ao executar arquivos/scripts em lote. Eis um exemplo de um arquivo em lote:

```
eshell start batch "&" set password plain <suasenha> "&" set status disabled
```

Este comando concatenado acima inicia um modo de lote, define a senha que será usada e desativa a proteção.

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

`[get] | restore password`

`set password [plain <senha>]`

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou limpar a senha

`restore` - Limpar a senha

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`senha` - Senha

EXEMPLOS:

`set password plain <suasenha>` - Define uma senha que será usada para comandos protegidos por senha

`restore password` - Limpa a senha

EXEMPLOS:

`get password` - Use este comando para ver se a senha está configurada (isto apenas exibe asteriscos "*", não lista a senha em si), quando não forem exibidos asteriscos, significa que não há uma senha definida

`set password plain <suasenha>` - Use para definir a senha definida

`restore password` - Este comando limpa a senha definida

STATUS

Exibir informações sobre o status atual de proteção do ESET File Security (similar à GUI).

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

`[get] | restore status`

`set status disabled | enabled`

OPERAÇÕES:

`get` - Exibir o status da proteção antivírus

`set` - Ativar/Desativar a proteção antivírus

`restore` - Restaura as configurações padrão

ARGUMENTOS:

`disabled` - Desativar a proteção antivírus

`enabled` - Ativar a proteção antivírus

EXEMPLOS:

`get status` - Exibe o status de proteção atual

`set status disabled` - Desativa a proteção

`restore status` - Restaura a proteção às configurações padrão (ativada)

VIRLOG

Este é um alias do comando `DETECTIONS` . É útil para visualizar informações sobre infiltrações detectadas.

WARNLOG

Este é um alias do comando `EVENTS` . É útil para visualizar informações sobre vários eventos.

4.10.2.1 Contexto - AV

ANTISTEALTH

Ativar o Anti-Stealth.

SINTAXE:

```
[get] | restore antistealth
```

```
set antistealth disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

CLEANLEVEL

Nível de limpeza.

SINTAXE:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não limpar

`normal` - Limpeza padrão

`strict` - Limpeza rígida

EXCLUSIONS

Exclusões.

SINTAXE:

```
[get] | clear exclusions
```

```
add | remove exclusions <exclusão>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`exclusion` - Arquivo/pasta/máscara excluído

EXTENSIONS

Extensões rastreadas/excluídas.

SINTAXE:

```
[get] | restore extensions
```

```
add | remove extensions <extensão> | /all | /extless
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`extension` - Extensão

`all` - Todos os arquivos

`extless` - Arquivos sem extensão

SELFDEFENSE

Autodefesa.

SINTAXE:

```
[get] | restore selfdefense
```

```
set selfdefense disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

STATUS

Status da proteção antivírus.

SINTAXE:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAÇÕES:

`get` - Exibir o status da proteção antivírus

`set` - Ativar/Desativar a proteção antivírus

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativar a proteção antivírus

`enabled` - Ativar a proteção antivírus

4.10.2.2 Contexto - AV DOCUMENT

CLEANLEVEL

Nível de limpeza.

SINTAXE:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não limpar

`normal` - Limpeza padrão

`strict` - Limpeza rígida

EXTENSIONS

Extensões rastreadas/excluídas.

SINTAXE:

```
[get] | restore extensions
```

```
add | remove extensions <extensão> | /all | /extless
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`extension` - Extensão

`all` - Todos os arquivos

`extless` - Arquivos sem extensão

INTEGRATION

Integrar a proteção de documentos ao sistema.

SINTAXE:

```
[get] | restore integration
```

```
set integration disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

STATUS

Status atual da proteção de documentos.

SINTAXE:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.3 Contexto - AV DOCUMENT LIMITS ARCHIVE

LEVEL

Nível de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
```

```
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível, de 1 a 20, ou 0 para usar as configurações padrão

SIZE

Tamanho máximo do arquivo no arquivo compactado (kB).

SINTAXE:

```
[get] | restore size
```

```
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB (1 - 3145728), ou 0 para usar as configurações padrão

4.10.2.4 Contexto - AV DOCUMENT LIMITS OBJECTS

SIZE

Tamanho máximo do arquivo (kB)

SINTAXE:

```
[get] | restore size
```

```
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB (1 - 3145728), ou 0 para usar as configurações padrão

TIMEOUT

Tempo máximo do rastreamento para arquivos (s)

SINTAXE:

```
[get] | restore timeout
```

```
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo em segundos (1 - 3600), ou 0 para usar as configurações padrão

4.10.2.5 Contexto - AV DOCUMENT OBJECTS

ARCHIVE

Rastrear arquivos.

SINTAXE:

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BOOT

Rastrear setores de inicialização.

SINTAXE:

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EMAIL

Rastrear arquivos de email.

SINTAXE:

```
[get] | restore email
```

```
set email disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

FILE

Rastrear arquivos.

SINTAXE:

```
[get] | restore file
```

```
set file disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MEMORY

Rastrear memória.

SINTAXE:

```
[get] | restore memory
set memory disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear compactadores em tempo real.

SINTAXE:

```
[get] | restore runtime
set runtime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de auto-extracção.

SINTAXE:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.6 Contexto - AV DOCUMENT OPTIONS

ADVHEURISTICS

Usar heurística avançada.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

ADWARE

Detecção de Adware/Spyware/Riskware.

SINTAXE:

```
[get] | restore adware
set adware disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HEURISTICS

Usar heurística.

SINTAXE:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SIGNATURES

Usar assinaturas.

SINTAXE:

```
[get] | restore signatures
set signatures disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNSAFE

Detecção de aplicativos potencialmente inseguros.

SINTAXE:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNWANTED

Detecção de aplicativos potencialmente não desejados.

SINTAXE:

```
[get] | restore unwanted
set unwanted disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.7 Contexto - AV DOCUMENT OTHER

LOGALL

Registrar todos os objetos.

SINTAXE:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPTIMIZE

Otimização inteligente.

SINTAXE:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.8 Contexto - AV EMAIL

ACTION

Ação para mensagens infectadas.

SINTAXE:

```
[get] | restore action
```

```
set action none | delete | movedeleted | moveto
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Nenhuma ação

`delete` - Excluir mensagem

`movedeleted` - Mover para excluídos

`moveto` - Mover para a pasta

CLIENTS

Clientes de email.

SINTAXE:

```
[get] clients
```

```
add | remove clients <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`path` - Caminho dos aplicativos

OBSERVAÇÃO: Ao filtrar apenas por aplicativo, você deve especificar quais aplicativos funcionam como clientes de email. Se um aplicativo não estiver marcado como cliente de email, o email poderá não ser rastreado.

QUARANTINE

Pasta de mensagens infectadas.

SINTAXE:

```
[get] | restore quarantine
```

```
set quarantine <string>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome da pasta

STATUS

Status da proteção do cliente de email.

SINTAXE:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.9 Contexto - AV EMAIL GENERAL

CLEANLEVEL

Nível de limpeza.

SINTAXE:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não limpar

`normal` - Limpeza padrão

`strict` - Limpeza rígida

EXTENSIONS

Extensões rastreadas/excluídas.

SINTAXE:

```
[get] | restore extensions
add | remove extensions <extensão> | /all | /extless
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`extension` - Extensão

`all` - Todos os arquivos

`extless` - Arquivos sem extensão

4.10.2.10 Contexto - AV EMAIL GENERAL LIMITS ARCHIVE

LEVEL

Nível de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível, de 1 a 20, ou 0 para usar as configurações padrão

SIZE

Tamanho máximo do arquivo no arquivo compactado (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

4.10.2.11 Contexto - AV EMAIL GENERAL LIMITS OBJECTS

SIZE

Tamanho máximo do arquivo (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

TIMEOUT

Tempo máximo do rastreamento para arquivos (s).

SINTAXE:

```
[get] | restore timeout
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo, em segundos, ou 0 para usar as configurações padrão

4.10.2.12 Contexto - AV EMAIL GENERAL OBJECTS

ARCHIVE

Rastrear arquivos.

SINTAXE:

```
[get] | restore archive
set archive disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BOOT

Rastrear setores de inicialização.

SINTAXE:

```
[get] | restore boot
set boot disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EMAIL

Rastrear arquivos de email.

SINTAXE:

```
[get] | restore email
set email disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

FILE

Rastrear arquivos.

SINTAXE:

```
[get] | restore file
set file disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MEMORY

Rastrear memória.

SINTAXE:

```
[get] | restore memory
set memory disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear compactadores em tempo real.

SINTAXE:

```
[get] | restore runtime
set runtime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de auto-extracção.

SINTAXE:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.13 Contexto - AV EMAIL GENERAL OPTIONS

ADVHEURISTICS

Usar heurística avançada.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

ADWARE

Detecção de Adware/Spyware/Riskware.

SINTAXE:

```
[get] | restore adware
set adware disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HEURISTICS

Usar heurística.

SINTAXE:

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SIGNATURES

Usar assinaturas.

SINTAXE:

```
[get] | restore signatures
```

```
set signatures disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNSAFE

Detecção de aplicativos potencialmente inseguros.

SINTAXE:

```
[get] | restore unsafe
```

```
set unsafe disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNWANTED

Detecção de aplicativos potencialmente não desejados.

SINTAXE:

```
[get] | restore unwanted
```

```
set unwanted disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.14 Contexto - AV EMAIL GENERAL OTHER

LOGALL

Registrar todos os objetos.

SINTAXE:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPTIMIZE

Otimização inteligente.

SINTAXE:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.15 Contexto - AV EMAIL MESSAGE CONVERT PLAIN

Converter o corpo do email em texto simples.

SINTAXE:

```
[get] | restore plain
set plain disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.16 Contexto - AV EMAIL MODIFY TEMPLATE

Modelo adicionado ao assunto das mensagens infectadas.

SINTAXE:

```
[get] | restore template
set template [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Texto

4.10.2.17 Contexto - AV EMAIL MODIFY RECEIVED BODY

Acrescentar mensagem nos emails recebidos e lidos.

SINTAXE:

```
[get] | restore body
set body never | infected | all
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`never` - Não adicionar

`infected` - Somente para mensagens infectadas

`all` - Para todas as mensagens

SUBJECT

Acrescentar observação ao assunto do email infectado recebido e enviado.

SINTAXE:

```
[get] | restore subject
```

```
set subject disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.18 Contexto - AV EMAIL MODIFY SENT

BODY

Acrescentar mensagem nos emails recebidos e lidos.

SINTAXE:

```
[get] | restore body
```

```
set body never | infected | all
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`never` - Não adicionar

`infected` - Somente para mensagens infectadas

`all` - Para todas as mensagens

SUBJECT

Acrescentar observação ao assunto do email infectado recebido e enviado.

SINTAXE:

```
[get] | restore subject
```

```
set subject disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.19 Contexto - AV EMAIL OEXPRESS/WINMAIL

INTEGRATION

Integrar ao Outlook Express e ao Windows Mail.

SINTAXE:

```
[get] | restore integration
set integration disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.20 Contexto - AV EMAIL OUTLOOK

FORCEADDIN

Usar complemento COM em versões mais antigas do Microsoft Outlook.

SINTAXE:

```
[get] | restore forceaddin
set forceaddin 2010newer | 2007newer | allversions
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`2010newer` - Miscrosoft Outlook 2010 e posteriores

`2007newer` - Miscrosoft Outlook 2007 e posteriores

`allversions` - Todas as versões do Microsoft Outlook

INTEGRATION

Integrar ao Microsoft Outlook.

SINTAXE:

```
[get] | restore integration
set integration disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SYNCFIX

Ativar a solução de conflitos de sincronização no Microsoft Outlook.

SINTAXE:

```
[get] | restore syncfix
```

```
set syncfix <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

`0` - Desativado. `3` - Totalmente ativado, outros valores possíveis.

4.10.2.21 Contexto - AV EMAIL OUTLOOK RESCAN ONCHANGE

Desativar verificação de alteração na caixa de entrada.

SINTAXE:

```
[get] | restore onchange
```

```
set onchange disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.22 Contexto - AV EMAIL PROTOCOL POP3 COMPATIBILITY

Configuração de compatibilidade.

SINTAXE:

```
[get] | restore compatibility
```

```
set compatibility compatible | both | effective
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`compatible` - Nível máximo de compatibilidade

`both` - Nível médio de compatibilidade

`effective` - Eficiência máxima

OBSERVAÇÃO: Nem todos os clientes de email funcionarão corretamente com a filtragem POP3 no modo padrão. As configurações a seguir permitem o ajuste do nível de compatibilidade para solucionar possíveis conflitos. No entanto, o aumento do nível de compatibilidade pode levar a uma redução da eficiência do monitor de Internet, ou na incapacidade de aproveitar todos os seus recursos.

PORTS

Portas utilizadas pelo POP3.

SINTAXE:

```
[get] | restore ports
```

```
set ports [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Números de porta separados por vírgulas

USE

Verificar POP3.

SINTAXE:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.23 Contexto - AV EMAIL PROTOCOL POP3S

COMPATIBILITY

Configuração de compatibilidade.

SINTAXE:

```
[get] | restore compatibility
```

```
set compatibility compatible | both | effective
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`compatible` - Nível máximo de compatibilidade

`both` - Nível médio de compatibilidade

`effective` - Eficiência máxima

OBSERVAÇÃO: Nem todos os clientes de email funcionarão corretamente com a filtragem POP3S no modo padrão. As configurações a seguir permitem o ajuste do nível de compatibilidade para solucionar possíveis conflitos. No entanto, o aumento do nível de compatibilidade pode levar a uma redução da eficiência do monitor de Internet, ou na incapacidade de aproveitar todos os seus recursos.

MODE

Modo de filtragem POP3S.

SINTAXE:

```
[get] | restore mode
```

```
set mode none | ports | clients
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não utilizar a verificação de protocolo POP3

`ports` - Utilizar a verificação de protocolo POP3S para as portas selecionadas

`clients` - Utilizar a verificação de protocolo POP3S para aplicativos marcados como clientes de email que utilizam as portas selecionadas

PORTS

Portas utilizadas pelo POP3S.

SINTAXE:

```
[get] | restore ports
```

```
set ports [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Números de porta separados por vírgulas

4.10.2.24 Contexto - AV EMAIL RESCAN

ONUPDATE

Repetir o rastreamento após atualização.

SINTAXE:

```
[get] | restore onupdate
set onupdate disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.25 Contexto - AV EMAIL SCAN

OTHERMODULES

Aceitar resultados de rastreamento de outros módulos.

SINTAXE:

```
[get] | restore othermodules
set othermodules disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

PLAIN

Rastrear o corpo do email em texto simples.

SINTAXE:

```
[get] | restore plain
set plain disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

READ

Rastrear mensagens lidas.

SINTAXE:

```
[get] | restore read
```

```
set read disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RECEIVED

Rastrear mensagens recebidas.

SINTAXE:

```
[get] | restore received
```

```
set received disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RTF

Rastrear o corpo do email em RTF.

SINTAXE:

```
[get] | restore rtf
```

```
set rtf disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SENT

Rastrear mensagens enviadas.

SINTAXE:

```
[get] | restore sent
set sent disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.26 Contexto - AV EMAIL THUNDERBIRD INTEGRATION

Integrar ao Mozilla Thunderbird.

SINTAXE:

```
[get] | restore integration
set integration disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.27 Contexto - AV EMAIL WINLIVE INTEGRATION

Integrar ao Windows Live Mail.

SINTAXE:

```
[get] | restore integration
set integration disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.28 Contexto - AV LIMITS ARCHIVE

LEVEL

Nível de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
```

```
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível, de 1 a 20, ou 0 para usar as configurações padrão

SIZE

Tamanho máximo do arquivo no arquivo compactado (kB).

SINTAXE:

```
[get] | restore size
```

```
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

4.10.2.29 Contexto - AV LIMITS OBJECTS

SIZE

Tamanho máximo do arquivo (kB).

SINTAXE:

```
[get] | restore size
```

```
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

TIMEOUT

Tempo máximo do rastreamento para arquivos (s).

SINTAXE:

```
[get] | restore timeout
```

```
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo, em segundos, ou O para usar as configurações padrão

4.10.2.30 Contexto - AV NETFILTER

AUTOSTART

Executar filtragem de conteúdo do protocolo de aplicativos HTTP e POP3 automaticamente.

SINTAXE:

```
[get] | restore autostart
```

```
set autostart disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EXCLUDED

Aplicativos excluídos da filtragem de protocolo.

SINTAXE:

```
[get] excluded
```

```
add | remove excluded <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`path` - Caminho dos aplicativos

MODE

Redirecionar tráfego para filtragem.

SINTAXE:

```
[get] | restore mode
```

```
set mode ports | application | both
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`ports` - Portas HTTP e POP3

`application` - Aplicativos marcados como navegadores da Internet ou clientes de email

`both` - Portas e aplicativos marcados como navegadores da Internet ou clientes de email

STATUS

Ativar filtragem de conteúdo do protocolo de aplicativos HTTP e POP3.

SINTAXE:

```
[get] | restore status
set status disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.31 Contexto - AV NETFILTER PROTOCOL SSL

BLOCKSSL2

Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2.

SINTAXE:

```
[get] | restore blockssl2
set blockssl2 disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EXCEPTIONS

Aplicar exceções criadas com base em certificados.

SINTAXE:

```
[get] | restore exceptions
set exceptions disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MODE

Modo de filtragem SSL.

SINTAXE:

```
[get] | restore mode
```

```
set mode allways | ask | none
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`allways` - Sempre usar a verificação SSL

`ask` - Perguntar sobre sites não visitados (exclusões podem ser definidas)

`none` - Não utilizar a verificação de protocolo SSL

4.10.2.32 Contexto - AV NETFILTER PROTOCOL SSL CERTIFICATE

ADDTOBROWSERS

Adicionar o certificado raiz aos navegadores conhecidos.

SINTAXE:

```
[get] | restore addtobrowsers
```

```
set addtobrowsers disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OBSERVAÇÃO: Para verificar corretamente o tráfego criptografado por SSL, o certificado raiz para ESET, spol. s r.o utilizado para assinar certificados será adicionado ao armazenamento de certificados de Autoridades de certificação raiz confiáveis (TRCA).

EXCLUDED

Lista de certificados excluídos da filtragem de conteúdo.

SINTAXE:

```
[get] excluded
remove excluded <nome>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`remove` - Remove o item

ARGUMENTOS:

`name` - Nome do certificado

NOTTRUSTED

Não confiável se o certificado for inválido ou estiver corrompido.

SINTAXE:

```
[get] | restore nottrusted
set nottrusted ask | block
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`ask` - Perguntar sobre validade do certificado

`block` - Bloquear a comunicação que utiliza o certificado

TRUSTED

Lista de certificados confiáveis.

SINTAXE:

```
[get] trusted
remove trusted <nome>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`remove` - Remove o item

ARGUMENTOS:

`name` - Nome do certificado

UNKNOWNROOT

Raiz desconhecida - caso o certificado não esteja validado por uma autoridade certificadora.

SINTAXE:

```
[get] | restore unknownroot
set unknownroot ask | block
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`ask` - Perguntar sobre validade do certificado

`block` - Bloquear a comunicação que utiliza o certificado

4.10.2.33 Contexto - AV OBJECTS

ARCHIVE

Rastrear arquivos.

SINTAXE:

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BOOT

Rastrear setores de inicialização.

SINTAXE:

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EMAIL

Rastrear arquivos de email.

SINTAXE:

```
[get] | restore email
```

```
set email disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MEMORY

Rastrear memória.

SINTAXE:

```
[get] | restore memory
```

```
set memory disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear compactadores em tempo real.

SINTAXE:

```
[get] | restore runtime
```

```
set runtime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de auto-extracção.

SINTAXE:

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.34 Contexto - AV OPTIONS

ADVHEURISTICS

Usar heurística avançada.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HEURISTICS

Usar heurística.

SINTAXE:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNSAFE

Detecção de aplicativos potencialmente inseguros.

SINTAXE:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNWANTED

Detecção de aplicativos potencialmente não desejados.

SINTAXE:

```
[get] | restore unwanted
```

```
set unwanted disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.35 Contexto - AV OTHER

LOGALL

Registrar todos os objetos.

SINTAXE:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPTIMIZE

Otimização inteligente.

SINTAXE:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.36 Contexto - AV REALTIME

AUTOSTART

Iniciar proteção em tempo real automaticamente.

SINTAXE:

```
[get] | restore autostart
set autostart disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

CLEANLEVEL

Nível de limpeza.

SINTAXE:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não limpar

`normal` - Limpeza padrão

`strict` - Limpeza rígida

EXTENSIONS

Extensões rastreadas/excluídas.

SINTAXE:

```
[get] | restore extensions
add | remove extensions <extensão> | /all | /extless
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`extension` - Extensão

`all` - Todos os arquivos

`extless` - Arquivos sem extensão

STATUS

Status da proteção do computador em tempo real.

SINTAXE:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.37 Contexto - AV REALTIME DISK

FLOPPY

Rastrear mídia removível.

SINTAXE:

```
[get] | restore floppy
```

```
set floppy disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

LOCAL

Rastrear unidades locais.

SINTAXE:

```
[get] | restore local
```

```
set local disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

NETWORK

Rastrear unidades de rede.

SINTAXE:

```
[get] | restore network
set network disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.38 Contexto - AV REALTIME EVENT

CREATE

Rastrear arquivos ao serem criados.

SINTAXE:

```
[get] | restore create
set create disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EXECUTE

Rastrear arquivos ao serem executados.

SINTAXE:

```
[get] | restore execute
set execute disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

FLOPPYACCESS

Rastrear ao acessar disquetes.

SINTAXE:

```
[get] | restore floppyaccess
set floppyaccess disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPEN

Rastrear arquivos ao serem abertos.

SINTAXE:

```
[get] | restore open
set open disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SHUTDOWN

Rastrear ao desligar o computador.

SINTAXE:

```
[get] | restore shutdown
set shutdown disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.39 Contexto - AV REALTIME EXECUTABLE

ADVHEURISTICS

Ativar heurística avançada na execução de arquivos.

SINTAXE:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.40 Contexto - AV REALTIME EXECUTABLE FROMREMOVABLE

ADVHEURISTICS

Ativar heurística avançada ao executar arquivos de mídia removível.

SINTAXE:

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EXCLUSION

Exclusões da unidade USB.

SINTAXE:

```
[get] | restore exclusion
```

```
select exclusion none | <unidade> | all
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`select` - Seleciona o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Desmarcar todas as unidades

`drive` - Letra da unidade a marcar/desmarcar

`all` - Selecionar todas as unidades

OBSERVAÇÃO: Use esta opção para permitir exceções no rastreamento usando heurística avançada na execução do arquivo. As configurações de heurística avançada para as unidades de disco rígido serão aplicadas aos dispositivos selecionados.

4.10.2.41 Contexto - AV REALTIME LIMITS ARCHIVE

LEVEL

Nível de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
```

```
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível, de 1 a 20, ou 0 para usar as configurações padrão

SIZE

Tamanho máximo do arquivo no arquivo compactado (kB).

SINTAXE:

```
[get] | restore size
```

```
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

4.10.2.42 Contexto - AV REALTIME LIMITS OBJECTS

SIZE

Tamanho máximo do arquivo (kB).

SINTAXE:

```
[get] | restore size
```

```
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

TIMEOUT

Tempo máximo do rastreamento para arquivos (s).

SINTAXE:

```
[get] | restore timeout
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo, em segundos, ou 0 para usar as configurações padrão

4.10.2.43 Contexto - AV REALTIME OBJECTS

ARCHIVE

Rastrear arquivos.

SINTAXE:

```
[get] | restore archive
set archive disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BOOT

Rastrear setores de inicialização.

SINTAXE:

```
[get] | restore boot
set boot disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EMAIL

Rastrear arquivos de email.

SINTAXE:

`[get] | restore email`

`set email disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MEMORY

Rastrear memória.

SINTAXE:

`[get] | restore memory`

`set memory disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear compactadores em tempo real.

SINTAXE:

`[get] | restore runtime`

`set runtime disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de auto-extracção.

SINTAXE:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.44 Contexto - AV REALTIME ONWRITE

ADVHEURISTICS

Ativar heurística avançada para arquivos novos e modificados.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear arquivos compactados do tempo de execução novos e modificados.

SINTAXE:

```
[get] | restore runtime
set runtime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de autoextração novos e modificados.

SINTAXE:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.45 Contexto - AV REALTIME ONWRITE ARCHIVE

LEVEL

Profundidade de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível (0 a 20)

SIZE

Tamanho máximo do arquivo no arquivo compactado rastreado (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho (kB)

4.10.2.46 Contexto - AV REALTIME OPTIONS

ADVHEURISTICS

Usar heurística avançada.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HEURISTICS

Usar heurística.

SINTAXE:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNSAFE

Detecção de aplicativos potencialmente inseguros.

SINTAXE:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNWANTED

Detecção de aplicativos potencialmente não desejados.

SINTAXE:

```
[get] | restore unwanted
set unwanted disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.47 Contexto - AV REALTIME OTHER

LOGALL

Registrar todos os objetos.

SINTAXE:

```
[get] | restore logall
set logall disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPTIMIZE

Otimização inteligente.

SINTAXE:

```
[get] | restore optimize
set optimize disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.48 Contexto - AV REALTIME REMOVABLE

BLOCK

Bloquear mídia removível.

SINTAXE:

```
[get] | restore block
```

```
set block disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EXCLUSION

Mídia removível permitida.

SINTAXE:

```
[get] | restore exclusion
```

```
select exclusion none | <unidade> | all
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`select` - Seleciona o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Desmarcar todas as unidades

`drive` - Letra da unidade a marcar/desmarcar

`all` - Selecionar todas as unidades

OBSERVAÇÃO: Use esta opção para habilitar o acesso a mídia removível (CD, disquetes, unidades USB). A seleção de uma mídia resulta na remoção das restrições de acesso ao tentar acessar essa mídia específica.

4.10.2.49 Contexto - AV WEB

BROWSERS

Navegadores da Internet.

SINTAXE:

```
[get] browsers
```

```
add | remove browsers <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`path` - Caminho dos aplicativos

OBSERVAÇÃO: Para aumentar a segurança, recomendamos que marque qualquer aplicativo usado como navegador de Internet selecionando a caixa correspondente. Se um aplicativo não for marcado como navegador de Internet, os dados transferidos usando esse aplicativo não serão rastreados.

CLEANLEVEL

Nível de limpeza.

SINTAXE:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não limpar

`normal` - Limpeza padrão

`strict` - Limpeza rígida

EXTENSIONS

Extensões rastreadas/excluídas.

SINTAXE:

```
[get] | restore extensions
```

```
add | remove extensions <extensão> | /all | /extless
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`extension` - Extensão

`all` - Todos os arquivos

`extless` - Arquivos sem extensão

STATUS

Proteção do acesso à web.

SINTAXE:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.50 Contexto - AV WEB ADDRESSMGMT

ADDRESS

Gerenciamento de endereços na lista selecionada.

SINTAXE:

```
[get] | clear address

add | remove address <address>

import | export address <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`importar` - Importa do arquivo

`export` - Exporta para um arquivo

`clear` - Remove todos os itens/arquivos

ARGUMENTOS:

`address` - Endereço

`path` - Caminho do arquivo

LIST

Gerenciamento da lista de endereços.

SINTAXE:

```
[get] | restore list

set list <nomelista> disabled | enabled

select | remove list <nomelista>

add list allowed <nomelista> | blocked <nomelista> | excluded <nomelista>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`select` - Selecionar para edição

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`listname` - Nome da lista

`disabled` - Não usar lista

`enabled` - Usar lista

`allowed` - Lista de endereços permitidos

`blocked` - Lista de endereços bloqueados

`excluded` - Lista de endereços excluídos da filtragem

OBSERVAÇÃO: Para editar a lista selecionada (marcada com - x), use o comando `av web addressmgmt address` .

NOTIFY

Notificar ao aplicar endereço da lista.

SINTAXE:

```
[get] | restore notify
```

```
set notify disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

WHITELISTED

Permitir acesso apenas a endereços HTTP na lista de endereços permitidos.

SINTAXE:

```
[get] | restore whitelisted
```

```
set whitelisted disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.51 Contexto - AV WEB LIMITS ARCHIVE

LEVEL

Nível de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
```

```
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível, de 1 a 20, ou 0 para usar as configurações padrão

SIZE

Tamanho máximo do arquivo no arquivo compactado (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

4.10.2.52 Contexto - AV WEB LIMITS OBJECTS

SIZE

Tamanho máximo do arquivo (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

TIMEOUT

Tempo máximo do rastreamento para arquivos (s).

SINTAXE:

```
[get] | restore timeout
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo, em segundos, ou 0 para usar as configurações padrão

4.10.2.53 Contexto - AV WEB OBJECTS

ARCHIVE

Rastrear arquivos.

SINTAXE:

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BOOT

Rastrear setores de inicialização.

SINTAXE:

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EMAIL

Rastrear arquivos de email.

SINTAXE:

```
[get] | restore email
```

```
set email disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

FILE

Rastrear arquivos.

SINTAXE:

```
[get] | restore file
set file disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MEMORY

Rastrear memória.

SINTAXE:

```
[get] | restore memory
set memory disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear compactadores em tempo real.

SINTAXE:

```
[get] | restore runtime
set runtime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de auto-extracção.

SINTAXE:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.54 Contexto - AV WEB OPTIONS

ADVHEURISTICS

Usar heurística avançada.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

ADWARE

Detecção de Adware/Spyware/Riskware.

SINTAXE:

```
[get] | restore adware
set adware disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HEURISTICS

Usar heurística.

SINTAXE:

```
[get] | restore heuristics
```

`set heuristics disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SIGNATURES

Usar assinaturas.

SINTAXE:

`[get] | restore signatures`

`set signatures disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNSAFE

Detecção de aplicativos potencialmente inseguros.

SINTAXE:

`[get] | restore unsafe`

`set unsafe disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNWANTED

Detecção de aplicativos potencialmente não desejados.

SINTAXE:

`[get] | restore unwanted`

`set unwanted disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.55 Contexto - AV WEB OPTIONS BROWSERS

ACTIVEMODE

Modo ativo para navegadores da Internet.

SINTAXE:

```
[get] activemode
```

```
add | remove activemode <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`path` - Caminho dos aplicativos

OBSERVAÇÃO: Programas adicionados à lista são automaticamente adicionados à lista de navegadores de Internet.

4.10.2.56 Contexto - AV WEB OTHER

LOGALL

Registrar todos os objetos.

SINTAXE:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPTIMIZE

Otimização inteligente.

SINTAXE:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.57 Contexto - AV WEB PROTOCOL HTTP

PORTS

Portas utilizadas por HTTP.

SINTAXE:

```
[get] | restore ports
set ports [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Números de portas separados por dois pontos

USE

Rastrear HTTP.

SINTAXE:

```
[get] | restore use
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.58 Contexto - AV WEB PROTOCOL HTTPS

MODE

Modo de filtragem HTTPS.

SINTAXE:

```
[get] | restore mode
```

```
set mode none | ports | browsers
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não utilizar a verificação de protocolo

`ports` - Utilizar a verificação de protocolo HTTPS para as portas selecionadas

`browsers` - Utilizar a verificação de protocolo HTTPS para aplicativos marcados como navegadores que utilizam as portas selecionadas

PORTS

Portas usadas pelo protocolo HTTPS.

SINTAXE:

```
[get] | restore ports
```

```
set ports [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Números de porta separados por vírgulas

4.10.2.59 Contexto - GENERAL

CONFIG

Importar/exportar configurações.

SINTAXE:

```
import | export config <caminho>
```

OPERAÇÕES:

`importar` - Importa do arquivo

`export` - Exporta para um arquivo

ARGUMENTOS:

`path` - Caminho do arquivo

LICENSE

Gerenciamento da licença.

SINTAXE:

```
[get] license
import license <caminho>
export license <ID> <caminho>
remove license <ID>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`remove` - Remove o item

`importar` - Importa do arquivo

`export` - Exporta para um arquivo

ARGUMENTOS:

`path` - Caminho do arquivo de licença

`ID` - ID da licença

4.10.2.60 Contexto - GENERAL ACCESS

ADMIN

Proteção das configurações dos direitos de administrador.

SINTAXE:

```
[get] | restore admin
set admin disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BATCH

Executar os comandos inseridos como argumentos quando o eShell estiver em execução.

SINTAXE:

```
[get] | restore batch
set batch disabled | <hora> | allways
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativado

`time` - Intervalo de tempo em minutos (1 a 1440 minutos)

`sempre` - Sempre

SENHA

Esta senha é utilizada para comandos protegidos por senha. Geralmente, para executar comandos protegidos por senha, você é solicitado a digitá-la. Isso ocorre por motivos de segurança. Aplica-se a comandos como os que desativam a proteção antivírus e os que podem afetar os recursos do ESET File Security. Será solicitada uma senha sempre que executar um desses comandos. Alternativamente, você pode definir esta senha para a sessão atual do eShell e não será necessário digitá-la novamente. Para obter mais detalhes, clique aqui.

Para inserir a senha sempre (recomendado), deixe os parâmetros em branco. Para redefinir a senha, digite uma senha em branco.

CAMINHO DO CONTEXTO:

`acesso geral`

SINTAXE:

`[get] | restore | set password`

OPERAÇÕES:

`get` - Exibir senha

`set` - Configurar senha

`restore` - Redefinir senha

EXEMPLOS:

`get password` - Use este comando para ver se a senha está configurada (isto apenas exibe asteriscos "*", não lista a senha em si), quando não forem exibidos asteriscos, significa que não há uma senha definida

`set password` - Use este comando para definir uma senha, simplesmente digite a senha (se nenhuma senha for inserida, a das configurações não será utilizada)

`restore password` - Este comando limpa a senha existente (a proteção das configurações não será usada)

EQUIVALENTE DA GUI:

clique aqui para ver como configurar isto pela GUI

4.10.2.61 Contexto - GENERAL ESHELL

ALIAS

Gerenciamento de alias.

SINTAXE:

`[get] | clear | restore alias`

`add alias [.] <alias>=<comando>`

`remove alias <alias>`

`import | export alias <caminho>`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`importar` - Importa do arquivo

`export` - Exporta para um arquivo

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`.` - Criar alias global

`alias` - Novo alias

`command` - Comando associado (validade do comando não verificada)

`alias` - Alias a excluir

`path` - Caminho do arquivo

LISTER

Usar criador de listas.

SINTAXE:

```
[get] | restore lister
```

```
set lister disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.62 Contexto - GENERAL ESHELL COLOR

ALIAS

Cor do alias.

SINTAXE:

```
[get] | restore alias
```

```
set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

COMMAND

Cor do comando.

SINTAXE:

```
[get] | restore command
```

```
set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

CONTEXT

Cor do contexto.

SINTAXE:

```
[get] | restore context
```

```
set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

DEFAULT

Cor básica.

SINTAXE:

```
[get] | restore default
```

```
set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

DISABLED

Cor de desativado.

SINTAXE:

```
[get] | restore disabled

set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan |
red | magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

ERROR

Cor das mensagens de erro.

SINTAXE:

```
[get] | restore error

set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red |
magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

INTERACTIVE

Cor das operações interativas.

SINTAXE:

```
[get] | restore interactive

set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan |
red | magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

LIST1

Cor da lista 1.

SINTAXE:

```
[get] | restore list1
```

```
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red |
magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

LIST2

Cor da lista 2.

SINTAXE:

```
[get] | restore list2
```

```
set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red |
magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

SUCCESS

Cor do status OK.

SINTAXE:

```
[get] | restore success
```

```
set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

WARNING

Cor das mensagens de aviso.

SINTAXE:

```
[get] | restore warning

set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`black` - Preto

`navy` - Azul marinho

`grass` - Verde bandeira

`ltblue` - Azul claro

`brown` - Marrom

`purple` - Roxo

`olive` - Verde oliva

`ltgray` - Cinza claro

`gray` - Cinza

`blue` - Azul

`green` - Verde

`cyan` - Ciano

`red` - Vermelho

`magenta` - Magenta

`yellow` - Amarelo

`white` - Branco

4.10.2.63 Contexto - GENERAL ESHELL OUTPUT

UTF8

Saída codificada em UTF8.

SINTAXE:

```
[get] | restore utf8
set utf8 disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OBSERVAÇÃO: Para exibir corretamente, a linha de comando deve usar uma fonte TrueType, como "Lucida Console".

4.10.2.64 Contexto - GENERAL ESHELL STARTUP

LOADCOMMANDS

Carregar todos os comandos na incialização.

SINTAXE:

```
[get] | restore loadcommands
set loadcommands disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

STATUS

Exibir status de proteção na inicialização.

SINTAXE:

```
[get] | restore status
set status disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.65 Contexto - GENERAL ESHELL VIEW

CMDHELP

Exibir ajuda em caso de falha de comando.

SINTAXE:

```
[get] | restore cmdhelp
set cmdhelp disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

COLORS

Usar cores.

SINTAXE:

```
[get] | restore colors
set colors disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

FITWIDTH

Cortar texto para ajustar à largura.

SINTAXE:

```
[get] | restore fitwidth
set fitwidth disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

GLOBAL

Exibir comandos globais.

SINTAXE:

```
[get] | restore global
set global disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HIDDEN

Exibir comandos ocultos.

SINTAXE:

```
[get] | restore hidden
set hidden disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPERATIONS

Exibir operações na lista de comandos.

SINTAXE:

```
[get] | restore operations
set operations disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SHORTLIST

Exibir lista de comandos abreviados ao alterar o contexto.

SINTAXE:

```
[get] | restore shortlist
set shortlist disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SYNTAXHINT

Exibir dicas de sintaxe do comando.

SINTAXE:

```
[get] | restore syntaxhint
set syntaxhint disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

VALUESONLY

Exibir apenas valores sem descrição.

SINTAXE:

```
[get] | restore valuesonly
set valuesonly disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.66 Contexto - GENERAL PERFORMANCE

SCANNERS

Quantidade de rastreamentos em execução.

SINTAXE:

```
[get] | restore scanners
```

```
set scanners <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Contagem (1 a 20)

4.10.2.67 Contexto - GENERAL PROXY

ADDRESS

Endereço do servidor proxy.

SINTAXE:

```
[get] | restore address
```

```
set address [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço

DETECT

Detecta as configurações do servidor proxy.

SINTAXE:

```
detect
```

LOGIN

Nome de login.

SINTAXE:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

SENHA

Senha do servidor proxy.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`senha` - Senha

PORT

Porta

SINTAXE:

```
[get] | restore port
```

```
set port <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Número da porta

USE

Usar servidor proxy.

SINTAXE:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.68 Contexto - GENERAL QUARANTINE RESCAN

UPDATE

Rastrear arquivos em quarentena após cada atualização.

SINTAXE:

```
[get] | restore update
```

```
set update disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

restore - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.69 Contexto - GENERAL REMOTE

INTERVAL

Intervalo da conexão (minutos).

SINTAXE:

```
[get] | restore interval
```

```
set interval <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo em minutos (1 a 1440)

USE

Conexão do servidor ERA.

SINTAXE:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.70 Contexto - GENERAL REMOTE SERVER PRIMARY

ADDRESS

Endereço do servidor ERA.

SINTAXE:

```
[get] | restore address
```

```
set address [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço

ENCRYPT

Bloquear conexão não criptografada.

SINTAXE:

```
[get] | restore encrypt
```

```
set encrypt disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SENHA

Senha do servidor ERA.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`senha` - Senha

PORT

Porta do servidor ERA.

SINTAXE:

```
[get] | restore port
```

```
set port <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Número da porta

4.10.2.71 Contexto - GENERAL REMOTE SERVER SECONDARY

ADDRESS

Endereço do servidor ERA.

SINTAXE:

```
[get] | restore address
```

```
set address [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço

ENCRYPT

Bloquear conexão não criptografada.

SINTAXE:

```
[get] | restore encrypt
```

```
set encrypt disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

PASSWORD

Senha do servidor ERA.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`senha` - Senha

PORT

Porta do servidor ERA.

SINTAXE:

```
[get] | restore port
```

```
set port <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Número da porta

4.10.2.72 Contexto - GENERAL TS.NET

EXCLUSION

Excluir do envio.

SINTAXE:

```
[get] | restore exclusion
```

```
add | remove exclusion <exclusão>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`exclusion` - Extensão

FROM

Email de contato.

SINTAXE:

```
[get] | restore from
```

```
set from [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço de email

LOGING

Criação de relatório.

SINTAXE:

[get] | restore loging

set loging disabled | enabled

OPERAÇÕES:

get - Retorna as configurações/status atuais

set - Define o valor/status

restore - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

disabled - Desativa a função/desativa as configurações

enabled - Ativa a função/Ativa as configurações

SENDING

Envio de arquivos suspeitos.

SINTAXE:

```
[get] | restore sending
set sending none | ask | auto
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não enviar

`ask` - Confirmar antes de enviar para análise

`auto` - Enviar para análise sem confirmação

VIA

Meios de envio de arquivo.

SINTAXE:

```
[get] | restore via
set via auto | ra | direct
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`auto` - Através do Administrador Remoto ou diretamente para a ESET

`ra` - Através do Administrador Remoto

`direct` - Diretamente para a ESET

WHEN

Quando enviar arquivos suspeitos.

SINTAXE:

```
[get] | restore when
```

```
set when asap | update
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`asap` - O mais breve possível

`atualizar` - Durante a atualização

4.10.2.73 Contexto - GENERAL TS.NET STATISTICS

SENDING

Envio de informações estatísticas.

SINTAXE:

```
[get] | restore sending
```

```
set sending disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

WHEN

Envio de informações estatísticas anônimas.

SINTAXE:

```
[get] | restore when
```

```
set when asap | update
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`asap` - O mais breve possível

`update` - Durante a atualização

4.10.2.74 Contexto - SCANNER

CLEANLEVEL

Nível de limpeza.

SINTAXE:

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não limpar

`normal` - Limpeza padrão

`strict` - Limpeza rígida

EXTENSIONS

Extensões rastreadas/excluídas.

SINTAXE:

```
[get] | restore extensions
```

```
add | remove extensions <extensão> | /all | /extless
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`extension` - Extensão

`all` - Todos os arquivos

`extless` - Arquivos sem extensão

PROFILE

Gerenciamento do perfil de rastreamento do computador.

SINTAXE:

```
[get] profile
```

```
select | remove profile <nome>
```

```
add profile new: <nome> [copyfrom: <nome>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`select` - Seleciona o item

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`name` - Nome do perfil

`new` - Novo perfil

`copyfrom` - Copiar configurações do perfil

OBSERVAÇÃO: Outros comandos de contexto referem-se ao perfil ativo (marcado com - x). Para selecionar o perfil ativo, use `select scanner profile <nome do perfil>`.

SCAN

Rastreamento do computador.

SINTAXE:

```
[get] | clear scan

start scan [readonly]

pause | resume | stop scan <ID> | all
```

OPERAÇÕES:

`get` - Exibir rastreamentos em execução e concluídos

`start` - Executar rastreamento do computador para o perfil selecionado

`stop` - Parar rastreamento

`resume` - Continuar rastreamento pausado

`pause` - Pausar rastreamento

`clear` - Remover rastreamentos concluídos da lista

ARGUMENTOS:

`readonly` - Rastrear sem limpar

`ID` - ID de rastreamento para a execução do comando

`all` - Executar comando para todos os rastreamentos

TARGET

Alvos de rastreamento para o perfil ativo.

SINTAXE:

```
[get] target

add | remove target <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`path` - Alvo/Caminho do rastreamento

OBSERVAÇÃO: Para rastrear o setor de inicialização, digite `X:\${Boot}` em que 'x' é o nome do disco rastreado.

4.10.2.75 Contexto - SCANNER LIMITS ARCHIVE

LEVEL

Nível de compactação de arquivos compactados.

SINTAXE:

```
[get] | restore level
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Nível, de 1 a 20, ou 0 para usar as configurações padrão

SIZE

Tamanho máximo do arquivo no arquivo compactado (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

4.10.2.76 Contexto - SCANNER LIMITS OBJECTS

SIZE

Tamanho máximo do arquivo (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho, em kB, ou 0 para usar as configurações padrão

TIMEOUT

Tempo máximo do rastreamento para arquivos (s).

SINTAXE:

```
[get] | restore timeout
```

```
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tempo, em segundos, ou 0 para usar as configurações padrão

4.10.2.77 Contexto - SCANNER OBJECTS

ARCHIVE

Rastrear arquivos.

SINTAXE:

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

BOOT

Rastrear setores de inicialização.

SINTAXE:

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

EMAIL

Rastrear arquivos de email.

SINTAXE:

```
[get] | restore email
set email disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

MEMORY

Rastrear memória.

SINTAXE:

```
[get] | restore memory
set memory disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

RUNTIME

Rastrear compactadores em tempo real.

SINTAXE:

```
[get] | restore runtime
set runtime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SFX

Rastrear arquivos compactados de auto-extracção.

SINTAXE:

```
[get] | restore sfx
set sfx disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.78 Contexto - SCANNER OPTIONS

ADVHEURISTICS

Usar heurística avançada.

SINTAXE:

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HEURISTICS

Usar heurística.

SINTAXE:

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNSAFE

Detecção de aplicativos potencialmente inseguros.

SINTAXE:

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

UNWANTED

Detecção de aplicativos potencialmente não desejados.

SINTAXE:

```
[get] | restore unwanted
```

```
set unwanted disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.79 Contexto - SCANNER OTHER

ADS

Rastrear fluxos dados alternativos (ADS).

SINTAXE:

```
[get] | restore ads
```

```
set ads disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

LOGALL

Registrar todos os objetos.

SINTAXE:

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

LOWPRIORITY

Executar rastreamento em segundo plano com baixa prioridade.

SINTAXE:

```
[get] | restore lowpriority
```

```
set lowpriority disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

OPTIMIZE

Otimização inteligente.

SINTAXE:

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

PRESERVETIME

Manter último registro de acesso.

SINTAXE:

```
[get] | restore preservetime
```

```
set preservetime disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SCROLL

Rolar relatório de rastreamento.

SINTAXE:

```
[get] | restore scroll
```

```
set scroll disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.80 Contexto - SERVER

AUTOEXCLUSIONS

Gerenciamento de exclusões automáticas.

SINTAXE:

```
[get] | restore autoexclusions
```

```
select autoexclusions <servidor>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`select` - Seleciona o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`server` - Nome do servidor

4.10.2.81 Contexto - TOOLS

QUARANTINE

Quarentena.

SINTAXE:

```
[get] quarantine
```

```
add quarantine <caminho>
```

```
send | remove | restore quarantine <ID>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

`send` - Envia o item/arquivo

ARGUMENTOS:

`path` - Caminho do arquivo

`ID` - ID do arquivo em quarentena

STATISTICS

Estatísticas.

SINTAXE:

```
[get] | clear statistics
```

OPERAÇÕES:

`get` - Exibir estatísticas

`clear` - Redefinir estatísticas

SYSINSPECTOR

SysInspector.

SINTAXE:

```
[get] sysinspector
add | remove sysinspector <nome>
export sysinspector <nome> to:<caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`export` - Exporta para um arquivo

ARGUMENTOS:

`name` - Comentário

`path` - Nome do arquivo (.zip ou .xml)

4.10.2.82 Contexto - TOOLS ACTIVITY

FILESYSTEM

Atividade do sistema de arquivos.

SINTAXE:

```
[get] filesystem [<contagem>] [seconds | minutes | hours [<ano>-<mês>]]
```

ARGUMENTOS:

`count` - Quantidade de registros a exibir

`seconds` - Amostragem de 1 segundo

`minutes` - Amostragem de 1 minuto

`hours` - Amostragem de 1 hora

`year` - Exibição até o ano atual

`month` - Exibição até o mês atual

4.10.2.83 Contexto - TOOLS LOG

DETECTIONS

Útil para visualizar informações sobre infiltrações detectadas.

CAMINHO DO CONTEXTO:

`raiz`

SINTAXE:

```
[get] detections [count <número>] [from <ano>-<mês>-<dia> <hora>:<minuto>:<segundo>] [to <ano>-<mês>-<dia> <hora>:<mi
```

`clear detections`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`clear` - Remove todos os itens/arquivos

ARGUMENTOS:

`count` - Exibe a quantidade selecionada de registros

`number` - Quantidade de registros

`from` - Exibir registros da hora especificada

`year` - Ano

`month` - Mês

`day` - Dia

`hour` - Hora

`minute` - Minuto

`second` - Segundo

`to` - Exibir registros até a hora especificada

ALIASES:

`virlog`

EXEMPLOS:

`get detections from 2011-04-14 01:30:00` - Exibe todas as infiltrações detectadas após 14 de abril de 2011, às 01:30:00 (ao definir a data, é necessário adicionar uma hora para que o comando funcione corretamente)

`clear detections` - Limpa todo o relatório

EVENTS

Útil para visualizar informações sobre vários eventos.

SINTAXE:

```
[get] events [count <número>] [from <ano>-<mês>-<dia> <hora>:<minuto>:<segundo>] [to <ano>-<mês>-<dia> <hora>:
<minuto>:<segundo>]
```

`clear events`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`clear` - Remove todos os itens/arquivos

ARGUMENTOS:

`count` - Exibe a quantidade selecionada de registros

`number` - Quantidade de registros

`from` - Exibir registros da hora especificada

`year` - Ano

`month` - Mês

`day` - Dia

`hour` - Hora

`minute` - Minuto

`segundo` - Segundo

`to` - Exibir registros até a hora especificada

ALIASES:

`warnlog`

EXEMPLOS:

`get events from 2011-04-14 01:30:00` - Exibe todos os eventos ocorridos após 14 de abril de 2011, às 01:30:00 (ao definir a data, é necessário adicionar uma hora para que o comando funcione corretamente)

`clear events` - Limpa todo o relatório

FILTER

Detalhamento mínimo de eventos para exibir.

SINTAXE:

```
[get] | restore filter
```

```
set filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] [all]] [smart]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Nenhum registro

`critical` - Erros críticos

`errors` - Erros

`warnings` - Avisos

`informative` - Registros informativos

`diagnostic` - Registros de diagnóstico

`all` - Todos os registros

`smart` - Filtragem inteligente

RASTREAMENTOS

Relatório ou lista de relatórios do "rastreamento do computador".

SINTAXE:

```
[get] rastreamentos [id:<id>] [count:<número>] [from:<ano>-<mês>-<dia> <hora>:<minuto>:<segundo>] [to:<ano>-<mês>-<dia> <hora>:<minuto>:<segundo>]
```

```
clear scans
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`clear` - Remove todos os itens/arquivos

ARGUMENTOS:

`id` - Exibir detalhes do rastreamento do computador com ID

`id` - ID de rastreamento

`count` - Exibir apenas a quantidade selecionada de registros

`number` - Quantidade de registros

`from` - Exibir apenas registros desde a hora especificada

`year` - Ano

`month` - Mês

`day` - Dia

`hour` - Hora

`minute` - Minuto

`second` - Segundo

`to` - Exibir apenas registros desde a hora especificada

VERBOSITY

Detalhamento mínimo de registro em relatório.

SINTAXE:

```
[get] | restore verbosity

set verbosity critical | errors | warnings | informative | diagnostic
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`critical` - Erros críticos

`errors` - Erros

`warnings` - Avisos

`informative` - Registros informativos

`diagnostic` - Registros de diagnóstico

4.10.2.84 Contexto - TOOLS LOG CLEANING

TIMEOUT

Tempo de vida dos relatórios (dias).

SINTAXE:

```
[get] | restore timeout
```

```
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Dias (1 a 365)

USE

Exclusão de registros automática.

SINTAXE:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.85 Contexto - TOOLS LOG OPTIMIZE

LEVEL

Otimizar excedendo a quantidade de registros não utilizados (porcentagem).

SINTAXE:

```
[get] | restore level
```

```
set level <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Porcentagem de registros não utilizados (1 a 100)

AGORA

Otimiza imediatamente arquivos de protocolo.

SINTAXE:

`now`

A execução do comando pode demorar alguns minutos.

USE

Otimização de registros automática.

SINTAXE:

`[get] | restore use`

`set use disabled | enabled`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.86 Contexto - TOOLS NOTIFICATION

VERBOSITY

Detalhamento mínimo de notificações.

SINTAXE:

`[get] | restore verbosity`

`set verbosity critical | errors | warnings | informative | diagnostic`

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`critical` - Erros críticos

`errors` - Erros

`warnings` - Avisos

`informative` - Registros informativos

`diagnostic` - Registros de diagnóstico

4.10.2.87 Contexto - TOOLS NOTIFICATION EMAIL

FROM

Endereço de email dos remetentes.

SINTAXE:

```
[get] | restore from
```

```
set from [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço de email

LOGIN

Nome de login.

SINTAXE:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

PASSWORD

Senha.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`senha` - Senha

SERVER

Endereço do servidor SMTP.

SINTAXE:

```
[get] | restore server
set server [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço

TO

Endereço de email dos destinatários.

SINTAXE:

```
[get] | restore to
set to [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço de email

USE

Envio de eventos por email.

SINTAXE:

```
[get] | restore use
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.88 Contexto - TOOLS NOTIFICATION MESSAGE

ENCODING

Codificação das mensagens de aviso.

SINTAXE:

```
[get] | restore encoding
```

```
set encoding nolocal | localcharset | localencoding | ISO-2022-JP
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`nolocal` - Não utilizar os caracteres do alfabeto nacional

`localcharset` - Usar caracteres do alfabeto nacional

`localencoding` - Usar caracteres e codificação do alfabeto nacional

`ISO` - Usar a codificação ISO-2022-JP (apenas para a versão japonesa)

4.10.2.89 Contexto - TOOLS NOTIFICATION MESSAGE FORMAT

DETECTION

Formato das mensagens de aviso de ameaça.

SINTAXE:

```
[get] | restore detection
```

```
set detection [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Formato de mensagem

Opções de formato da mensagem:

`%TimeStamp%` - Data e hora do evento

`%Scanner%` - Módulo que detectou o evento

`%ComputerName%` - Nome do computador

`%ProgramName%` - Programa que causou o evento

`%ErrorDescription%` - Descrição do erro

Para obter o formato da mensagem, é necessário substituir as palavras-chave (listadas aqui entre os sinais de porcentagem "%") pelos valores correspondentes.

OBSERVAÇÃO: Os avisos e mensagens de vírus do ESET File Security têm um formato padrão. Não recomendamos alterar esse formato. Você pode alterar o formato caso esteja usando um sistema de envio automático de emails.

EVENT

Formato do evento.

SINTAXE:

```
[get] | restore event
```

```
set event [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Formato de mensagem

Opções de formato da mensagem:

`%TimeStamp%` - Data e hora do evento

`%Scanner%` - Módulo que detectou o evento

`%ComputerName%` - Nome do computador

`%ProgramName%` - Programa que causou o evento

`%InfectedObject%` - Objeto infectado (arquivo, e-mail, etc.)

`%VirusName%` - Nome do vírus

Para obter o formato da mensagem, é necessário substituir as palavras-chave (listadas aqui entre os sinais de porcentagem "%") pelos valores correspondentes.

OBSERVAÇÃO: Os avisos e mensagens de vírus do ESET File Security têm um formato padrão. Não recomendamos alterar esse formato. Você pode alterar o formato caso esteja usando um sistema de envio automático de emails.

4.10.2.90 Contexto - TOOLS NOTIFICATION WINPOPUP

ADDRESS

Envia notificações a nomes de computador.

SINTAXE:

```
[get] | restore address
```

```
set address [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome do computador, separados por uma vírgula

TIMEOUT

Intervalo de envio a computadores na rede.

SINTAXE:

```
[get] | restore timeout
```

```
set timeout <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Intervalo em segundos (1 a 3600)

USE

Enviar eventos a computadores na rede.

SINTAXE:

```
[get] | restore use
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.91 Contexto - TOOLS SCHEDULER

ACTION

Ação da tarefa agendada.

SINTAXE:

```
[get] action
set action external | logmaintenance | startupcheck | status | scan | update
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`external` - Executar aplicativo externo

`logmaintenance` - Manutenção de relatórios

`startupcheck` - Rastreamento na inicialização

`status` - Criar um instantâneo do status do computador

`rastreamento` - Rastrear o computador

`update` - Atualizar

TASK

Tarefas agendadas.

SINTAXE:

```
[get] | select task [<ID>]
set task <ID> disabled | enabled
```

```
add task <nome_tarefa>
remove | start task <ID>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`select` - Seleciona o item

`add` - Adicionar item

`remove` - Remove o item

`start` - Inicia a tarefa

ARGUMENTOS:

`ID` - ID da tarefa

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

`task_name` - Nome da tarefa

TRIGGER

Execução de tarefas.

SINTAXE:

```
[get] trigger
set trigger once | repeat | daily | weekly | event
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`once` - Uma vez

`repeat` - Repetidamente

`daily` - Diariamente

`weekly` - Semanalmente

`event` - Disparado por evento

4.10.2.92 Contexto - TOOLS SCHEDULER EVENT

INTERVAL

Executar tarefa somente uma vez no intervalo especificado (horas).

SINTAXE:

```
[get] interval
set interval <horas>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`hours` - Tempo em horas (1 a 720 horas)

TYPE

Tarefa acionada por evento.

SINTAXE:

```
[get] type
set type startup | startuponcedaily | dialup | engineupdate | appupdate | logon | detection
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`startup` - Na inicialização do computador

`startuponcedaily` - Na primeira vez em que o computador for iniciado diariamente

`dialup` - Ao fazer uma conexão dial-up com a Internet/VPN

`engineupdate` - Na atualização do banco de dados de assinatura de vírus

`appupdate` - Na atualização de componente do programa

`logon` - Após logon do usuário

`detecção` - Detecção de ameaças

4.10.2.93 Contexto - TOOLS SCHEDULER FAILSAFE

EXECUTE

Ação a realizar se a tarefa não for executada.

SINTAXE:

```
[get] execute
set execute asap | iftimeout | no
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`asap` - Executar a tarefa assim que possível

`iftimeout` - E&xecutar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado

`no` - Não executar com atraso

OBSERVAÇÃO: Para definir um limite, digite `SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT <HORAS>`.

TIMEOUT

Intervalo da tarefa (horas).

SINTAXE:

```
[get] timeout
set timeout <horas>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`hours` - Tempo em horas (1 a 720 horas)

4.10.2.94 Contexto - TOOLS SCHEDULER PARAMETERS CHECK

LEVEL

Nível de rastreamento.

SINTAXE:

```
[get] level
```

```
set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`before_logon` - Os arquivos são executados antes do logon do usuário

`after_logon` - Os arquivos são executados após o logon do usuário

`most_frequent` - Somente os arquivos mais frequentemente usados

`frequent` - Arquivos frequentemente usados

`common` - Arquivos comumente usados

`rare` - Arquivos raramente usados

`all` - Arquivos registrados

PRIORITY

Prioridade do rastreamento.

SINTAXE:

```
[get] priority
```

```
set priority [normal | low | lowest | idle]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`normal` - Normal

`low` - Mais baixa

`lowest` - A mais baixa possível

`idle` - Quando ocioso

4.10.2.95 Contexto - TOOLS SCHEDULER PARAMETERS EXTERNAL

ARGUMENTS

Argumentos.

SINTAXE:

```
[get] arguments
set arguments <argumentos>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`arguments` - Argumentos

DIRECTORY

Pasta de trabalho.

SINTAXE:

```
[get] directory
set directory <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`path` - Caminho

EXECUTABLE

Arquivo executável.

SINTAXE:

```
[get] executable
set executable <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`path` - Caminho

4.10.2.96 Contexto - TOOLS SCHEDULER PARAMETERS SCAN

PROFILE

Perfil de rastreamento.

SINTAXE:

```
[get] profile
```

```
set profile <perfil>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`perfil` - Nome do perfil

READONLY

Rastrear sem limpar.

SINTAXE:

```
[get] readonly
```

```
set readonly disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

TARGET

Alvos de rastreamento.

SINTAXE:

```
[get] | clear target
```

```
add | remove target <caminho>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`add` - Adicionar item

`remove` - Remove o item

`clear` - Remove todos os itens/arquivos

ARGUMENTOS:

`path` - Caminho/alvo do rastreamento

4.10.2.97 Contexto - TOOLS SCHEDULER PARAMETERS UPDATE

PRIMARY

Perfil de atualização.

SINTAXE:

```
[get] primary
```

```
set primary [<perfil>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`perfil` - Nome do perfil

SECONDARY

Perfil de atualização alternativo.

SINTAXE:

```
[get] secondary
```

```
set secondary [<perfil>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`perfil` - Nome do perfil

4.10.2.98 Contexto - TOOLS SCHEDULER REPEAT

INTERVAL

Intervalo da tarefa (minutos).

SINTAXE:

```
[get] interval
```

```
set interval <minutos>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`minutes` - Tempo em minutos (1 a 720 horas)

4.10.2.99 Contexto - TOOLS SCHEDULER STARTUP

DATE

A tarefa será executada na data selecionada.

SINTAXE:

```
[get] date
set date <ano>-<mês>-<dia>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`year` - Ano

`month` - Mês

`day` - Dia

DAYS

Executar a tarefa nos dias a seguir.

SINTAXE:

```
[get] days
set | add | remove days none | [monday] [tuesday] [wednesday] [thurdsday] [friday] [saturday] [sunday] | all
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`add` - Adiciona item

`remove` - Remove o item

ARGUMENTOS:

`none` - Sem dia especificado

`monday` - Segunda-feira

`tuesday` - Terça-feira

`wednesday` - Quarta-feira

`thurdsday` - Quinta-feira

`friday` - Sexta-feira

`saturday` - Sábado

`sunday` - Domingo

`all` - Todos os dias

TIME

A tarefa será executada na hora selecionada.

SINTAXE:

```
[get] time
set time <hora>:<minuto>:<segundo>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

ARGUMENTOS:

`hour` - Hora

`minute` - Minuto

`second` - Segundo

4.10.2.100 Contexto - UPDATE

CACHE

Limpar cache de atualização.

SINTAXE:

```
clear cache
```

COMPONENTS

Atualizar componentes do programa.

SINTAXE:

```
[get] | restore components
```

```
set components never | allways | ask
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`never` - Não atualizar

`allways` - Sempre atualizar

`ask` - Perguntar antes de atualizar os componentes do programa

LOGIN

Login do usuário.

SINTAXE:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

OBSERVAÇÃO: Insira o usuário e a senha recebidos após a aquisição ou ativação. Recomendamos que copie (Ctrl+C) as informações de seu email de registro e cole-as (Ctrl+V).

PASSWORD

Senha.

SINTAXE:

```
[get] | restore password
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou excluir a senha

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`password` - Senha

OBSERVAÇÃO: Insira o usuário e a senha recebidos após a aquisição ou ativação. Recomendamos que copie (Ctrl+C) as informações de seu email de registro e cole-as (Ctrl+V).

PRERELEASE

Ativar modo de teste.

SINTAXE:

```
[get] | restore prerelease
set prerelease disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

PROFILE

Gerenciamento do perfil de atualização.

SINTAXE:

```
[get] profile
select | remove profile <nome>
add profile new: <nome> [copyfrom: <nome>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`select` - Seleciona o item

`add` - Adicionar item

`remove` - Remove o item

ARGUMENTOS:

`name` - Nome do perfil

`new` - Novo perfil

`copyfrom` - Copiar configurações do perfil

OBSERVAÇÃO: Outros comandos de contexto referem-se ao perfil ativo (marcado com - x). Para selecionar o perfil ativo, use `select update profile <nome do perfil>`.

SERVER

Atualizar servidores.

SINTAXE:

```
[get] | restore server
```

```
select | add | remove server <servidor>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`select` - Seleciona o item

`add` - Adicionar item

`remove` - Remove o item

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`server` - Endereço do servidor

STATUS

Exibir status da atualização.

SINTAXE:

```
[get] status
```

UPDATE

Atualizar.

SINTAXE:

```
start | stop update
```

OPERAÇÕES:

`start` - Executar atualização

`stop` - Cancelar atualização

4.10.2.101 Contexto - UPDATE CONNECTION

DISCONNECT

Desconectar do servidor depois da atualização.

SINTAXE:

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

LOGIN

Nome de usuário.

SINTAXE:

```
[get] | restore login
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

PASSWORD

Senha.

SINTAXE:

```
[get] | restore password
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou excluir a senha

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`password` - Senha

RUNAS

Conectar na rede como.

SINTAXE:

```
[get] | restore runas
set runas system | current | specified
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`system` - Conta do sistema (padrão)

`current` - Usuário atual

`specified` - Usuário especificado

4.10.2.102 Contexto - UPDATE MIRROR

COMPONENTS

Atualizar componentes do programa.

SINTAXE:

```
[get] | start | restore components
set components disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`start` - Iniciar atualização

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

FOLDER

Pasta para armazenar arquivos da imagem.

SINTAXE:

```
[get] | restore folder
set folder [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Caminho da pasta

LOGIN

Nome de usuário.

SINTAXE:

```
[get] | restore login
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

PASSWORD

Senha.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou excluir a senha

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`password` - Senha

USE

Criar imagem da atualização.

SINTAXE:

```
[get] | restore use
```

```
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

VERSIONS

Gerenciamento da versão de atualização.

SINTAXE:

```
[get] | restore versions
```

```
select versions <versão>
```

OPERAÇÕES:

`get` - Exibir versões disponíveis

`select` - Marcar/Desmarcar versão de atualização

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`version` - Nome da versão

4.10.2.103 Contexto - UPDATE MIRROR CONNECTION

DISCONNECT

Desconectar do servidor depois da atualização.

SINTAXE:

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

LOGIN

Nome de usuário.

SINTAXE:

```
[get] | restore login
```

```
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

PASSWORD

Senha.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou excluir a senha

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`password` - Senha

RUNAS

Conectar na rede como.

SINTAXE:

```
[get] | restore runas
set runas system | current | specified
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`system` - Conta do sistema (padrão)

`current` - Usuário atual

`specified` - Usuário especificado

4.10.2.104 Contexto - UPDATE MIRROR SERVER

AUTHENTICATION

Usar autenticação.

SINTAXE:

```
[get] | restore authentication
set authentication none | basic | ntlm
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`none` - Não

`basic` - Básico

`ntlm` - NTLM

PORT

Porta.

SINTAXE:

```
[get] | restore port
set port <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Número da porta

USE

Fornecer arquivos de atualização através do servidor HTTP.

SINTAXE:

```
[get] | restore use
set use disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

4.10.2.105 Contexto - UPDATE NOTIFICATION

DOWNLOAD

Perguntar antes de fazer download da atualização.

SINTAXE:

```
[get] | restore download
set download disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

HIDE

Não exibir notificação sobre atualização bem-sucedida.

SINTAXE:

```
[get] | restore hide
set hide disabled | enabled
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`disabled` - Desativa a função/desativa as configurações

`enabled` - Ativa a função/Ativa as configurações

SIZE

Perguntar se um arquivo de atualização for maior que (kB).

SINTAXE:

```
[get] | restore size
set size <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Tamanho do arquivo (kB)

OBSERVAÇÃO: Para desativar as notificações de atualização, digite `0`.

4.10.2.106 Contexto - UPDATE PROXY

LOGIN

Nome de usuário.

SINTAXE:

```
[get] | restore login
set login [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Nome

MODE

Configuração do proxy HTTP.

SINTAXE:

```
[get] | restore mode
set mode global | noproxy | userdefined
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`global` - Usar configurações globais de servidor proxy

`noproxy` - Não usar servidor proxy

`userdefined` - Conexão através de um servidor proxy

PASSWORD

Senha.

SINTAXE:

```
[get] | restore password
```

```
set password [plain <senha>]
```

OPERAÇÕES:

`get` - Exibir senha

`set` - Definir ou excluir a senha

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`plain` - Alternar para inserir a senha como parâmetro

`password` - Senha

PORT

Porta do servidor proxy.

SINTAXE:

```
[get] | restore port
```

```
set port <número>
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`number` - Número da porta

SERVER

Servidor proxy.

SINTAXE:

```
[get] | restore server
```

```
set server [<string>]
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`string` - Endereço do servidor

4.10.2.107 Contexto - UPDATE SYSTEM

NOTIFY

Notificar sobre atualizações faltantes no nível.

SINTAXE:

```
[get] | restore notify
```

```
set notify no | optional | recommended | important | critical
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

`no` - Não

`optional` - Opcional

`recommended` - Recomendado

`important` - Importante

`critical` - Crítico

RESTART

Reiniciar o computador após uma atualização de componente do programa.

SINTAXE:

```
[get] | restore restart
```

```
set restart never | ask | auto
```

OPERAÇÕES:

`get` - Retorna as configurações/status atuais

`set` - Define o valor/status

`restore` - Restaura as configurações/objeto/arquivo padrão

ARGUMENTOS:

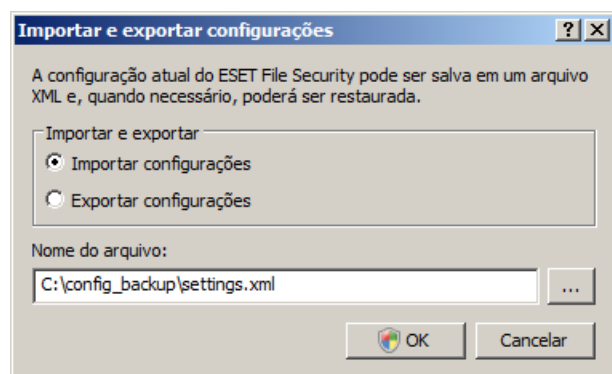
`never` - Não reiniciar

`ask` - Perguntar antes de reiniciar

`auto` - Reiniciar automaticamente

4.11 Importar e exportar configurações

A importação e a exportação de configurações do ESET File Security está disponível em **Configurar** clicando em **Importar e exportar configurações**.

Tanto a importação quanto a exportação utilizam arquivos .xml. A importação e a exportação serão úteis caso precise fazer backup da configuração atual do ESET File Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais do ESET File Security em diversos sistemas. Os usuários podem importar facilmente um arquivo .xml para transferir as configurações desejadas.

4.12 ThreatSense.Net

O ThreatSense.Net Early Warning System mantém a ESET contínua e imediatamente informada sobre novas infiltrações. O sistema de alerta bidirecional do ThreatSense.Net Early Warning System tem uma única finalidade: melhorar a proteção que podemos proporcionar-lhe. A melhor maneira de garantir que veremos novas ameaças assim que elas aparecerem é mantermos "link" com o máximo possível de nossos clientes e usá-los como nossos Sentinelas de ameaças. Há duas opções:

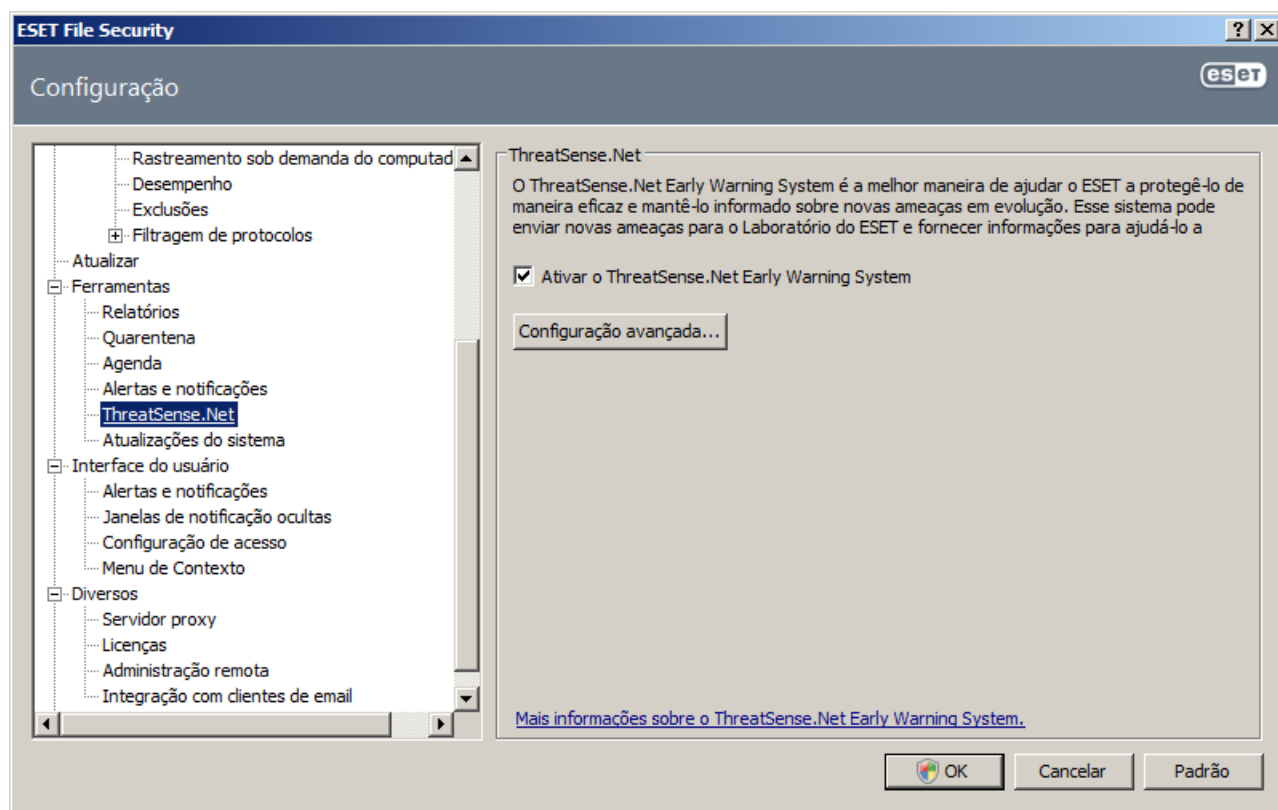
1. Você pode optar por não ativar o ThreatSense.Net Early Warning System. Você não perderá nenhuma funcionalidade do software e ainda receberá a melhor proteção que oferecemos.

2. É possível configurar o ThreatSense.Net Early Warning System para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ThreatSense.Net Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

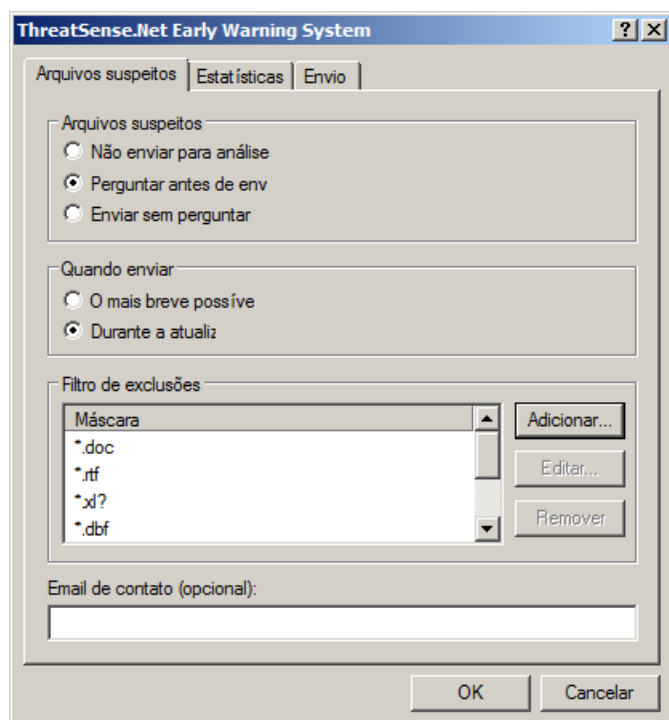
Enquanto há uma possibilidade de que isso possa ocasionalmente revelar algumas informações sobre você ou seu computador (usuários em um caminho de diretório, etc.) para o Laboratório de ameaças da ESET, essas informações não serão utilizadas para QUALQUER outra finalidade que não seja nos ajudar a reagir imediatamente contra novas ameaças.

Por padrão, o ESET File Security é configurado para perguntar antes de enviar arquivos suspeitos ao Laboratório de ameaças da ESET para análise detalhada. Os arquivos com certas extensões, como .doc ou .xls, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

A configuração do ThreatSense.Net pode ser acessada na árvore Configuração avançada, em **Ferramentas** > **ThreatSense.Net**. Selecione a opção **Ativar o ThreatSense Early Warning System** para ativá-lo e clique no botão **Configuração avançada...**

4.12.1 Arquivos suspeitos

A guia **Arquivos suspeitos** permite configurar a maneira como as ameaças serão enviadas ao Laboratório de ameaças da ESET para análise.

Se encontrar um arquivo suspeito, você poderá enviá-lo para análise no nosso Laboratório de ameaças. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

O envio de arquivos pode ser definido para ocorrer automaticamente ou selecione a opção **Perguntar antes de enviar**, se desejar saber quais arquivos foram enviados para análise e confirmar o envio.

Se não desejar que os arquivos sejam enviados, selecione a opção **Não enviar para análise**. A seleção da opção de não envio de arquivos para análise não influencia o envio das informações estatísticas, que são definidas em sua própria configuração. (consulte a seção Estatísticas).

Quando enviar - Por padrão, a opção **O mais breve possível** fica selecionada para que os arquivos suspeitos sejam enviados ao Laboratório de ameaças da ESET. Esta é a opção recomendada se uma conexão permanente com a Internet estiver disponível e os arquivos suspeitos puderem ser enviados sem atraso. Selecione a opção **Durante a atualização** para que o upload de arquivos suspeitos seja feito para o ThreatSense.Net durante a próxima atualização.

Filtro de exclusões – O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

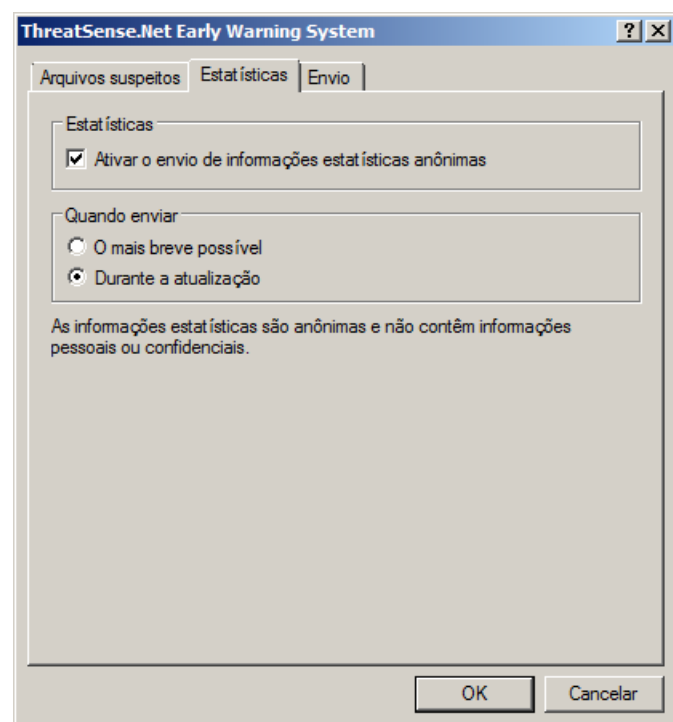
Email de contato – Seu **Email de contato (opcional)**pode ser enviado com qualquer arquivo suspeito e pode ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

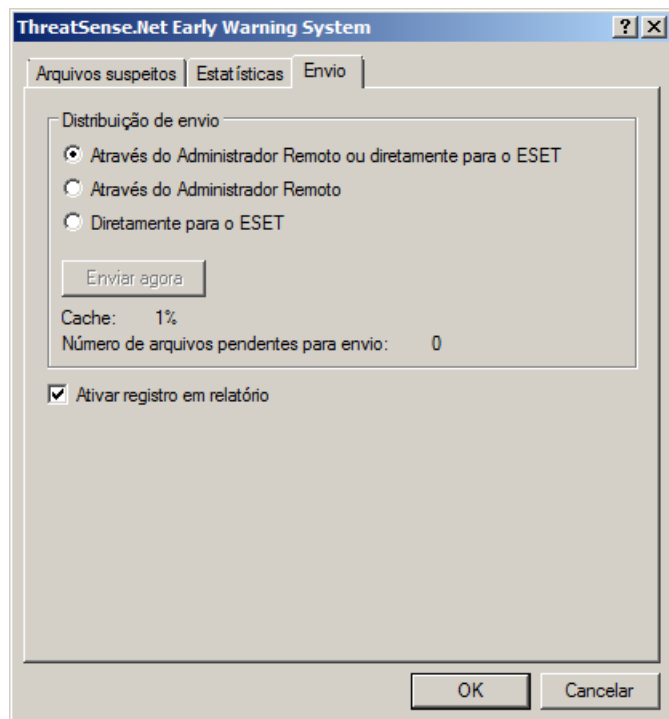
4.12.2 Estatísticas

O ThreatSense.Net Early Warning System coletará informações anônimas sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir o nome da ameaça, a data e o horário em que ela foi detectada, a versão do produto de segurança da ESET, a versão do seu sistema operacional e a configuração de local. As estatísticas são normalmente enviadas aos servidores da ESET, uma ou duas vezes por dia.

A seguir há um exemplo de um pacote estatístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

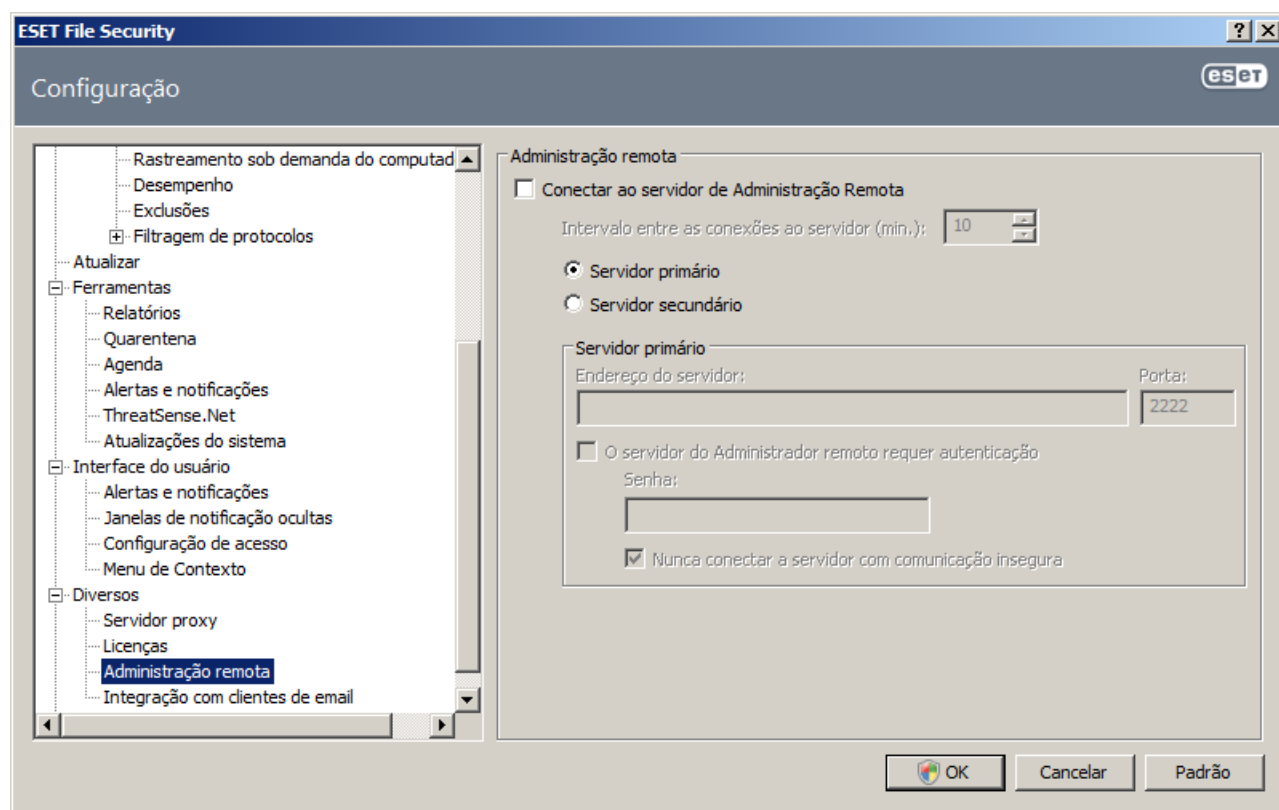
Quando enviar - Você pode definir o momento em que as informações estatísticas serão enviadas. Se optar por enviar **O mais breve possível**, as informações estatísticas serão enviadas imediatamente após serem criadas. Esta configuração é adequada se um conexão permanente com a Internet estiver disponível. Se a opção **Durante a atualização** estiver selecionada, todas as informações estatísticas serão enviadas em grupo durante a próxima atualização.

4.12.3 Envio

Você pode selecionar como os arquivos e as informações estatísticas serão enviados à ESET. Selecione a opção **Através do Administrador Remoto ou diretamente para a ESET** para enviar arquivos e estatísticas por qualquer meio disponível. Selecione a opção **Através do Administrador Remoto** para enviar os arquivos e as estatísticas ao servidor da administração remota, que assegurará o envio posterior ao Laboratório de ameaças da ESET. Se a opção **Diretamente para a ESET** estiver selecionada, todos os arquivos suspeitos e informações estatísticas serão enviados para o laboratório de vírus da ESET diretamente do programa.

Quando houver arquivos com envio pendente, o botão **Enviar agora** estará ativado. Clique nesse botão para enviar arquivos e informações estatísticas imediatamente.

Selecione a opção **Ativar registro em relatório** para criar um relatório para registrar os envios de arquivos e informações estatísticas.

4.13 Administração remota

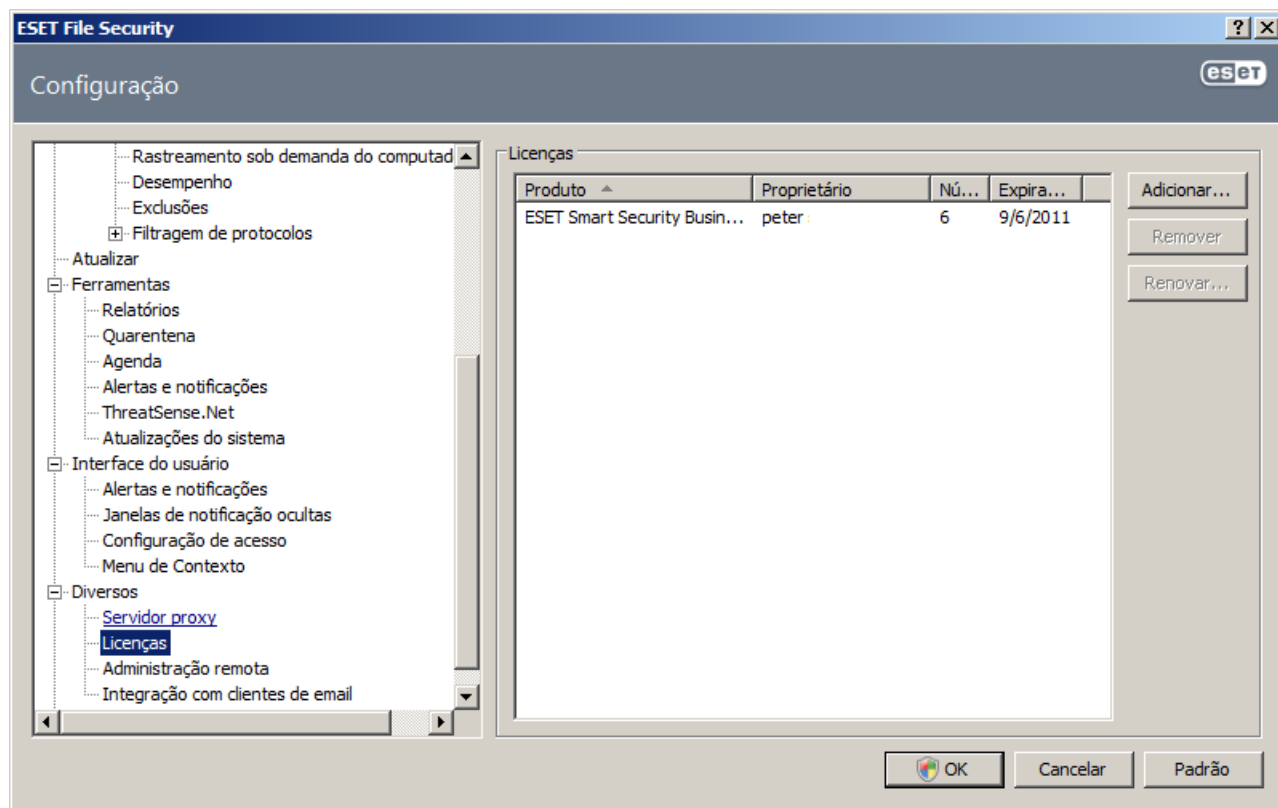
O ESET Remote Administrator (ERA) é uma ferramenta poderosa para gerenciar a política de segurança e para obter uma visão geral de toda a segurança em uma rede. É especialmente útil quando aplicada a redes maiores. O ERA não aumenta somente o nível de segurança, mas também fornece facilidade de uso no gerenciamento do ESET File Security em estações de trabalho clientes.

As opções de configuração de administração remota estão disponíveis na janela principal do programa ESET File Security. Clique em **Configuração (Setup)** > **Entrar na configuração avançada... (Enter the entire advanced setup tree...)** > **Diversos (Miscellaneous)** > **Administração remota (Remote administration)**.

Ative a administração remota selecionando a opção **Conectar ao servidor de Administração Remota (Connect to Remote Administration server)**. É possível acessar as outras opções descritas a seguir:

- **Intervalo entre as conexões ao servidor (min.) (Interval between connections to server (min.)):** Isso designa a frequência com que o ESET File Security se conectará ao servidor ERA. Se estiver configurado como 0, as informações serão enviadas a cada 5 segundos.
- **Endereço do servidor (Server address):** Endereço de rede do servidor em que o servidor ERA está instalado.
- **Porta:** Esse campo contém um valor predefinido utilizado para conexão. Recomendamos que você deixe a configuração de porta padrão em 2222
- **O servidor do Administrador remoto requer autenticação (Remote Administrator server requires authentication):** Permite inserir a senha para conexão com o servidor ERA, se necessário.

Clique em **OK** para confirmar as alterações e aplicar as configurações. O ESET File Security as usará para conectar-se ao servidor ERA.

4.14 Licenças

A ramificação **Licenças** permite gerenciar as chaves de licença do ESET File Security e de outros produtos da ESET, como a ESET Mail Security etc. Após a compra, as chaves de licença são fornecidas com o nome de usuário e a senha. Para **Adicionar/Remover** uma chave de licença, clique no botão correspondente na janela do gerenciador de licenças. O gerenciador de licenças pode ser acessado na árvore Configuração avançada em **Diversos** > **Licenças**.

A chave de licença é um arquivo de texto que contém informações sobre o produto comprado: o proprietário, o número de licenças e a data de expiração.

A janela do gerenciador de licenças permite fazer upload e visualizar o conteúdo de uma chave de licença usando o botão **Adicionar...** – as informações contidas serão exibidas no gerenciador. Para excluir os arquivos de licença da lista, clique em **Remover**.

Se uma chave de licença tiver expirado e você estiver interessado em adquirir a renovação, clique no botão **Solicitar...**; você será redirecionado à nossa loja on-line.

5. Glossário

5.1 Tipos de infiltrações

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

5.1.1 Vírus

Um vírus de computador é uma infiltração que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente depois disso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que o usuário, acidental ou deliberadamente, execute ou abra ele mesmo o programa malicioso.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositalmente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus (quando comparados a cavalos de troia ou spyware) estão se tornando cada vez mais raros, uma vez que eles não são comercialmente atrativos para os autores de softwares maliciosos. Além disso, o termo "vírus" é frequentemente usado de maneira incorreta para cobrir todos os tipos de infiltrações. Essa utilização está gradualmente sendo superada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador estiver infectado por um vírus, será necessário restaurar os arquivos infectados para o seu estado original, ou seja, limpá-los usando um programa antivírus.

Os exemplos de vírus são: OneHalf, Tenga, e Yankee Doodle.

5.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms são propagados por meio dos endereços de e-mail da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais férteis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas ou em até em minutos, após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversos transtornos: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Exemplos de worms bem conhecidos são: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

5.1.3 Cavalos de tróia (Trojans)

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de infiltração que tenta se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Mas é importante observar que isso era verdadeiro para os cavalos de troia do passado – hoje não há necessidade de eles se disfarçarem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não se encaixe em uma classe específica de infiltração.

Uma vez que essa é uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** – Um programa malicioso com a capacidade de fazer o download de outras infiltrações a partir da Internet
- **Dropper** – Um tipo de cavalo de troia desenvolvido para instalar outros tipos de softwares maliciosos em computadores comprometidos
- **Backdoor** – Um aplicativo que se comunica com os agressores remotos, permitindo que obtenham acesso ao sistema e assumam o controle dele
- **Keylogger** – (keystroke logger) – Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos
- **Dialer** – Dialers são programas desenvolvidos para se conectar aos números premium-rate. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modems discados que não são mais usados regularmente.

Os cavalos de troia geralmente tomam a forma de arquivos executáveis com extensão .exe. Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele quase sempre contém códigos maliciosos.

Os exemplos dos cavalos de troia bem conhecidos são: NetBus, Trojandownloader. Small.ZL, Slapper

5.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo em que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows, etc. Por este motivo, é quase impossível detectá-los usando técnicas de teste comuns.

Há dois níveis de detecção para impedir rootkits:

1) Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
2) Quando eles estão ocultos para os testes usuais. Os usuários do ESET File Security têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

5.1.5 Adware

Adware é a abreviação de advertising-supported software (software patrocinado por propaganda). Os programas que exibem material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a página inicial do navegador. O adware é frequentemente vinculado a programas freeware, permitindo que seus desenvolvedores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso — os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware também pode executar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa de instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Determinados programas não serão instalados sem o adware, ou as suas funcionalidades ficarão limitadas. Isso

significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há grande possibilidade de que contenha códigos maliciosos.

5.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de e-mail da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINS, números de contas bancárias, etc. O Spyware freqüentemente é vinculado a versões gratuitas de um programa pelo seu autor a fiim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

5.1.7 Aplicativos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET File Security fornece a opção de detectar tais ameaças.

"Aplicativos potencialmente inseguros" é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo potencialmente inseguro presente e sendo executado em seu computador (e que você não instalou), consulte o seu administrador de rede ou remova o aplicativo.

5.1.8 Aplicativos potencialmente indesejados

Aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o desempenho do computador. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- São abertas novas janelas que você não via anteriormente
- Ativação e execução de processos ocultos
- Uso aumentado de recursos do sistema
- Alterações nos resultados de pesquisa
- O aplicativo comunica-se com servidores remotos